NOTAS DE AULA

TEORIA DOS NÚMEROS

(Versão 01/06/2009)

Por

Benedito Tadeu Vasconcelos Freire

S U M Á R I O

Aula 1 – Noções sobre o processo e o método de indução

Apresentação

Esta é a primeira aula da disciplina Teoria dos Números, que pretende: introduz os resultados básicos da Teoria Elementar dos Números; mostra aplicações da Teoria dos Números; desenvolve mecanismos de reconhecimento de padrões numéricos; e introduz o rigor nas provas dos resultados.

Nesta primeira aula, introduziremos o processo e o método de indução, uma importante técnica usada para provar resultados em Matemática e especialmente na Teoria dos Números.

Tente entender tudo que está sendo explicado na aula. Estude com caneta e papel ao lado. Seja paciente e procure ter certeza de que você entendeu o que (e por que) está fazendo.

Objetivos

- Compreender a essência do processo indutivo.
- Usar o Princípio da Indução para provar a validade de certas fórmulas envolvendo números naturais.

O processo e o método indutivo

Em muitos problemas de Matemática, especialmente da Teoria dos Números, precisamos verificar a veracidade de uma afirmação, A(n), que depende de um número natural n. Se a afirmação A(n) é de fato verdadeira, usamos o método de indução para facilitar a sua prova. Os historiadores da Matemática têm opiniões diferentes sobre quem primeiro formulou o Princípio da Indução Matemática. Mas, é certo que os matemáticos da antiga Grécia usaram argumentos indutivos, basta ver o Teorema IX-20 em *Os Elementos*, de Euclides, onde ele prova a existência de infinitos números primos.

Atenção: ao longo de todas estas Notas de Aula, a letra maiúscula **N** denotará o conjunto dos números naturais:

N = {1, 2, 3, 4, 5, 6, ..., n, ...}.

A letra maiúscula **Z** denotará o conjunto dos números inteiros:

Z = {...., -3, -2, -1, 0, 1, 2, 3, 4, ...}

Euclides de Alexandria (360 a.C. — 295 a.C.) foi um professor, matemático e escritor. Teria sido educado em Atenas e freqüentado a Academia de Platão, em pleno florescimento da cultura helenística.

Convidado por Ptolomeu I para compor o quadro de professores da recém fundada Academia, que tornaria Alexandria o centro do saber da época, tornou-se o mais importante autor de matemática da Antiguidade greco-romana e talvez de todos os tempos, com seu monumental Stoichia (**Os elementos**, 300 a.C.), uma obra em treze volumes, sendo cinco sobre geometria plana, três sobre números, um sobre a teoria das proporções, um sobre incomensuráveis e os três últimos sobre geometria no espaço. Escrita em grego, a obra cobria toda a aritmética, a álgebra e a geometria conhecidas até então no mundo grego, reunindo o trabalho de seus predecessores, como Hipócrates e Eudóxio, e sistematizava todo o conhecimento geométrico dos antigos e intercalava os teoremas já conhecidos então com a demonstração de muitos outros, que completavam lacunas e davam coerência e encadeamento lógico ao sistema por ele criado. Após sua primeira edição foi copiado e recopiado inúmeras vezes e, versado para o árabe, tornou-se o mais influente texto científico de todos os tempos e um dos com maior número de publicações ao longo da história. Depois da queda do Império Romano, os seus livros foram recuperados para a sociedade européia pelos estudiosos árabes da península Ibérica. Escreveu ainda Óptica (295 a.C.), sobre a óptica da visão e sobre astrologia, astronomia, música e mecânica, além de outros livros sobre matemática. Entre eles citam-se Lugares de superfície, Pseudaria e Porismas.

Algumas das suas obras, como Os elementos, Os dados, outro livro de texto, uma espécie de manual de tabelas de uso interno na Academia e complemento dos seis primeiros volumes de Os Elementos, Divisão de figuras, sobre a divisão geométrica de figuras planas, Os Fenômenos, sobre astronomia, e Óptica, sobre a visão, sobreviveram parcialmente e hoje são, depois de A Esfera de Autólico, os mais antigos tratados científicos gregos existentes. Pela sua maneira de expor nos escritos deduz-se que tenha sido um habilíssimo professor.

(Fonte: WIKIPÉDIA, 2008, extraído da Internet).

Alguns historiadores argumentam que a formulação precisa do método e do processo de indução deveu-se a Jacob Bernoulli (1654-1705) e Blaise Pascal (1623 - 1662). Em 1889, quando estudava os números naturais, Giuseppe Peano (1858—1932) introduziu o Princípio da Indução Matemática como um dos axiomas dos números naturais.

Em que consiste o método de indução matemática?

A prova por indução pode ser pensada como a brincadeira de arrumar dominós em fila e derrubá-los como uma onda: derrubamos a primeira peça, que ao cair bate na segunda, que ao cair bate na terceira e assim por diante, até que todas elas estejam tombadas, conforme mostra a Figura 1.

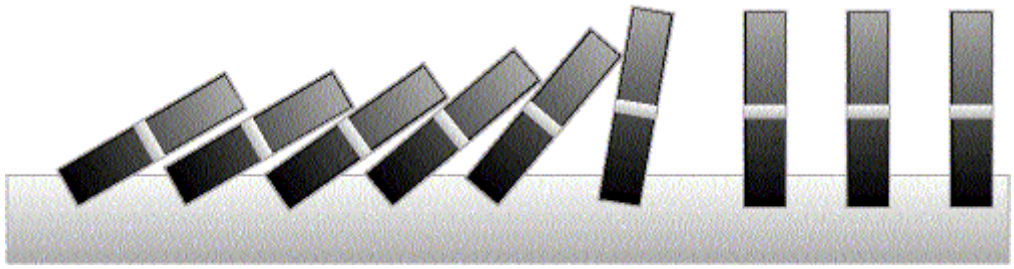

Figura 1 – Dominós caindo como uma onda

Agora, em vez de peças de dominós, pense numa seqüência de afirmações A (1), A (2), A (3), ..., A(n), ... Imagine que seja possível provar as duas etapas seguintes:

(i) a primeira afirmação, A (1), seja verdadeira;
(ii) sempre que uma afirmação for verdadeira, a imediatamente seguinte também seja verdadeira.

Concluímos que todas as afirmações A (1), A (2), A (3), ..., A(n), ... são verdadeiras.

Relacionando com as peças de dominó, (i) seria a derrubada da primeira peça, (ii) seria a queda de uma peça de dominó provocada pela queda da peça anterior.

A parte (i) é chamada a **base da indução** e (ii) é a **etapa indutiva**.

Exemplo 1 (A soma dos primeiros *n* números naturais)

Vamos provar, usando indução, que para todo número natural *n*, temos:

$$1+2+3+4+....+n=\frac{n(n+1)}{2}$$

Solução

Observe que a afirmação A(*n)* a ser provada é: $1+2+3+4+....+n=\frac{n(n+1)}{2}$, para cada número natural *n*.

Assim, A (1) será entendida como a afirmação: $1 = \frac{1.(1+1)}{2}$;

A (2) : $1+2 = \frac{2(2+1)}{2}$;

A (3): $1+2+3 = \frac{3(3+1)}{2}$, e assim por diante.

Etapa 1 – Vamos verificar a base da indução. Isto é, (i), que é o mesmo que verificar que A (1) é verdadeira. Para isso, basta observar que: $1 = \frac{1.(1+1)}{2}$.

Etapa 2 – Vamos supor que para $n = k$, onde k um número natural maior do que ou igual a 1, a fórmula dada seja verdadeira. Isto é, $1+2+3+4+...+k = \frac{k(k+1)}{2}$. Agora, provaremos que para $n = k+1$ a igualdade também se verifica. De fato, somando $k + 1$ em ambos os membros da expressão anterior, obtém-se

$$1+2+3+4+....+k+(k+1) = \frac{k(k+1)}{2} + (k+1) =$$

$$= (k+1).(\frac{k}{2}+1) = (k+1).(\frac{k+2)}{2}) = (k+1).\frac{[(k+1)+1]}{2},$$ que é o resultado $\frac{n(n+1)}{2}$ para n = k +1. Portanto, pelo Princípio da Indução, completamos a prova.

Exemplo 2 (A soma dos quadrados dos primeiros *n* números naturais)

Vamos provar por indução que, para todo número natural *n,* temos:

$$1^2 + 2^2 + 3^2 + 4^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Solução

A afirmação, A(*n)*, a ser provada é: $1^2 + 2^2 + 3^2 + 4^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$, para todo número natural *n.*

Assim, A (1) será entendida como a afirmação $\frac{1(1+1)(2.1+1)}{6} = 1^2 = 1$;

A (2): $1^2 + 2^2 = \frac{2(2+1)(2.2+1)}{6} = \frac{2.3.5}{6} = 5$;

A (3): $1^2 + 2^2 + 3^2 = \frac{3(3+1)(2.3+1)}{6} = 14$ e assim por diante.

Etapa 1 – Vai verificar a base da indução, isto é, (i). Para isso, basta observar que: $\frac{1(1+1)(2.1+1)}{6} = 1^2 = 1$.

Etapa 2 – Vamos supor que para $n = k$, onde k é um número natural maior do que ou igual a 1, a fórmula dada seja verdadeira. Isto é, $1^2 + 2^2 + 3^2 + 4^2 + ... + k^2 = \frac{k(k+1)(2k+1)}{6}$ para todo número natural k.

Agora, provaremos que para $n = k + 1$ a igualdade também se verifica. De fato, somando $(k+1)^2$ em ambos os membros da igualdade anterior, obtém-se:

$= (k+1)\left[\frac{2k^2 + k + 6k + 6}{6}\right] = (k+1).\left[\frac{2k^2 + 7k + 6}{6}\right] = \frac{(k+1)((k+2)[2(k+1)+1]}{6}$, esta é a expressão $\frac{n(n+1)(2n+1)}{6}$ quando $n = k + 1$, o que completa a prova.

Exercício 1

Descubra o erro na demonstração, por indução, do seguinte resultado:

Proposição - Todos os objetos possuem a mesma cor.

Demonstração

O caso n = 1 é óbvio (numa coleção consistindo de um único objeto, existe uma única cor a ser observada). Assumindo, por hipótese, que em qualquer coleção de k objetos todos têm a mesma cor, então, segue que toda coleção de k + 1 objetos será formada totalmente por elementos monocromáticos. De fato, se retirarmos um objeto de uma coleção de k + 1 objetos, os k restantes serão todos da mesma cor (pela hipótese). Agora, se colocamos de volta o que foi retirado e retiramos outro qualquer, então, (novamente) pela hipótese de indução, ele tem a mesma cor dos objetos restantes e, com isso, concluímos que todos os objetos possuem a mesma cor.

Exemplo 3 (A soma dos cubos dos primeiros *n* números naturais)

Vamos provar por indução que, para todo número natural *n, temos:*

$$1^3 + 2^3 + 3^3 + 4^3 + ... + n^3 = \left[\frac{n(n+1)}{2}\right]^2$$

Solução

A afirmação, A(*n)*, a ser provada é: $1^3 + 2^3 + 3^3 + 4^3 + ... + n^3 = \left[\frac{n(n+1)}{2}\right]^2$ para todo número natural *n.*

Assim, A (1) será entendida como a afirmação $1 = \left[\frac{1.(1+1)}{2}\right]^2$;

A (2): $1^3 + 2^3 = \left[\frac{2(2+1)}{2}\right]^2$;

A (3) : $1^3 + 2^3 + 3^3 = \left[\frac{3(3+1)}{2}\right]^2$, e assim por diante.

Etapa 1 – Vamos verificar a base da indução. Isto é, (i). Assim, vamos verificar que é verdadeira. Para isso, basta observar que: $1^3 = \left[\frac{1.(1+1)}{2}\right]^2 = \left[\frac{2}{2}\right]^2 = 1$.

Etapa 2 – Vamos supor que para $n = k$, onde k é um número natural maior do que ou igual a 1, a fórmula dada seja verdadeira. Isto é, $1^3 + 2^3 + 3^3 + 4^3 + ... + k^3 = \left[\frac{k(k+1)}{2}\right]^2$, para todo número natural k.

Agora, provaremos que para $n = k + 1$ a igualdade também se verifica. De fato,

$$1^3 + 2^3 + 3^3 + 4^3 + ... + k^3 + (k+1)^3 = \left[\frac{k(k+1)}{2}\right]^2 + (k+1)^3 = (k+1)^2\left[\frac{k^2}{4} + (k+1)\right] =$$

$$= (k+1)^2\left[\frac{k^2 + 4k + 4}{4}\right] = (k+1)^2.\left[\frac{k+2}{2}\right]^2 = \left[\frac{(k+1)(k+2)}{2}\right]^2,$$ que é a fórmula $\left[\frac{n(n+1)}{2}\right]^2$ para $n = k + 1$, o que completa a prova.

Observe que, pelo exemplo 1, temos $1 + 2 + 3 + 4 + ... + n = \frac{n(n+1)}{2}$. Agora, o exemplo 2, curiosamente, nos permite concluir que:

$$1^3 + 2^3 + 3^3 + 4^3 + ... + n^3 = \left[\frac{n(n+1)}{2}\right]^2 = (1 + 2 + 3 + 4 + ... + n)^2,$$

um resultado, convenhamos, surpreendente!

Exercício 2

Prove, por indução, que para todo número natural n, vale as seguintes igualdades:

(a) $\frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + ... + \frac{1}{(n-1).n} = \frac{n-1}{n}$

(b) $1 + x + x^2 + x^3 + ... + x^n = \frac{x^{n+1} - 1}{x - 1}$

(c) $\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right)\left(1 - \frac{1}{16}\right)...\left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}$

(d) $1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + ... + \frac{1}{2n+1} - \frac{1}{2n} = \frac{1}{n+1} + \frac{1}{n+2} + \frac{1}{n+3} + ... + \frac{1}{2n}$.

A Torre de Hanói

A Torre de Hanói é um quebra-cabeça que foi apresentado em 1883 por Édouard Lucas (1842-1891), um professor do Lycées Saint-Louis, na França, no seu livro *Récréations Mathématiques*, volume III, p. 56. Lucas anexou ao seu brinquedo uma lenda romântica sobre uma torre, a Torre de Brama, que supostamente tem 64 discos de ouro empilhados em três agulhas de diamantes:

"No início dos tempos", ele disse, "Deus colocou estes discos de ouro na primeira agulha e mandou um grupo de sacerdotes transferir para a terceira agulha, movendo apenas um disco de cada vez e sem colocar um disco maior em cima de um menor. Os sacerdotes, ao que se saiba, trabalham dia e noite nesta tarefa. Quando eles terminarem, a Torre ruirá e o mundo irá acabar".

A primeira solução do problema da Torre de Hanói apareceu na literatura matemática em 1884, num artigo de Allardice e Farser, La Tour d'Hanoi publicado em *Proc. Edinburgh Math. Soc*., v. 2, p. 50 – 53, 1884.

A seguir, enunciamos o problema da Torre de Hanói de forma mais geral.

Exemplo 4 (A Torre de Hanói)

É dada uma torre com n discos, inicialmente empilhados por tamanhos decrescentes em um dos três pinos dados, conforme Figura 2. O objetivo é transferir a torre inteira para um dos outros pinos, movendo apenas um disco de cada vez e sem colocar um disco maior em cima de um menor.

a) Determine a menor quantidade de movimentos necessários para transferir todos os discos de um dos pinos para outro.

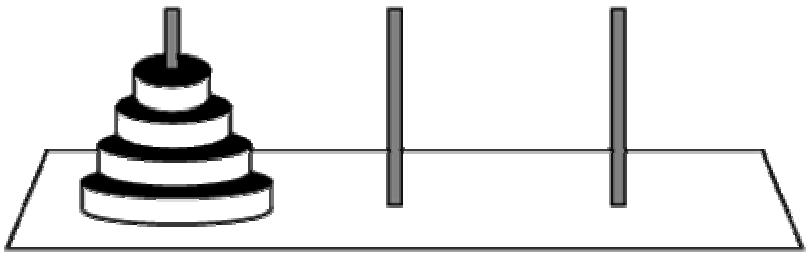

Figura 2 - A Torre de Hanói

b) **Mais precisamente**: prove que podemos realizar a transferência dos n discos, de acordo com as regras de Édouard Lucas, com, no mínimo, $2^n - 1$ movimentos.

Solução

a) Na nossa notação anterior, a afirmação, A(n), a ser provada é: "a menor quantidade de movimentos para transferir os n discos é igual a $2^n - 1$".

Assim, A (1) será entendida como a afirmação: "A quantidade mínima de movimentos para transferir um disco é igual a $2^1 - 1 = 1$";
A (2): a menor quantidade de movimentos para transferir dois discos é igual a $2^2 - 1$;
A (3): a menor quantidade de movimentos para transferir três discos é igual a $2^3 - 1$, e assim por diante.

Etapa 1 – Vamos verificar a base da indução. Ou seja, vamos verificar que A (1) é verdadeira. Para isso, observe que, para transferir um só disco, basta um único movimento. Nesse caso, $1 = 2^1 - 1$ e a fórmula se verifica.

Etapa 2 – Vamos supor que para $n = k$, onde k é o número de discos, a menor quantidade de movimentos para realizar a transferência seja $2^k - 1$. Naturalmente, k é um número natural maior do que ou igual a 1.

b) Agora, provaremos que, para $n = k + 1$ discos, o número mínimo de movimentos que realizam a transferência é dado por $2^{n+1} - 1$.
De fato, se temos $(k + 1)$ discos, podemos pensar em dois blocos de discos: um bloco com k discos, contendo todos os discos, com exceção do disco maior, que está embaixo da pilha, e outro, só com o disco maior. Pela hipótese de indução, podemos transferir os k primeiros discos com, no mínimo, $2^k - 1$ movimento. Assim, transferimos o bloco contendo k discos para um dos pinos vazios, realizando $2^k - 1$ movimentos e, em seguida, transferimos o disco maior para o outro pino vazio e, por último, transferimos o bloco dos k discos para o pino em que se encontra o disco maior, com no mínimo $2^k - 1$ movimentos. Em seguida, com um movimento transferimos o disco maior para o outro pino vazio. Portanto, o total mínimo de movimentos realizados foi:

$$(2^k - 1) + 1 + (2^k - 1) = 2.2^k - 1 = 2^{k+1} - 1, \text{ o que conclui a prova.}$$

No caso de n = 64 discos, o número mínimo de movimentos será $2^{64} - 1$, necessários antes que o mundo se acabe...
Agora, observe que o número $2^{64} - 1$ é igual a 18.446.744.073.709.551.615.
Se fizermos uma transferência por segundo, 24 horas por dia, durante 365 dias no ano, levaríamos 58.454.204.609 séculos e mais seis anos para terminar o trabalho!

É oportuno observar que a demonstração por indução exige que comprovemos que uma dada afirmação A(n) sobre números naturais seja verdadeira para $n = 1$. E, supondo verdadeira para n = k, possamos, através de meios legítimos, provarmos que ela seja verdadeira para $n = k + 1$. Somente após essas duas etapas, podemos concluir que A(n) é verdadeira para todo número natural n. Os dois exemplos a seguir ilustram bem o teor dessa observação.

Exemplo 5
A expressão $n^2 + n + 41$ representa um número primo para $n = 1, 2, 3, ..., 39$ (verifique essa afirmação, substituindo na expressão dada os valores: $n = 1$, n = 2, ..., n =39). Mas, para n = 40, temos:
$n^2 + n + 41 = 40^2 + 40 + 41 = 40(40 + 1) + 41 = 40 \times 41 + 41 = 41 \times 41 = 41^2$, que não é um número primo. Esse cálculo evidencia que a validade para $n = 39$ não implica a validade para $n = 40$. Esse é um exemplo famoso que foi dado por Leonardo Euler.

Exemplo 6
Suponha verdadeira a seguinte afirmação:

$$A(n) = 1 + 2 + 3 + 4 + ... + n = \frac{(n-1)(n+2)}{2}.$$

Então, a afirmação:

$$A(n+1) = (1 + 2 + 3 + 4 + ... + n) + n + 1 = \frac{(n-1)(n+2)}{2} + n + 1 =$$

$$= \frac{(n-1)(n+2)}{2} + \frac{2(n+1)}{2} = \frac{n^2 + n - 2 + 2n + 2}{2} = \frac{n^2 + 3n}{2} = \frac{n(n+3)}{2}$$

é verdadeira. Logo, a veracidade de A(n) implica a de A (n + 1). No entanto, A (1) = 1, enquanto $\frac{(n-1)(n+2)}{2} = 0$, para $n = 1$.

Isso nos diz que A (1) não é verdadeira. Portanto, não podemos concluir que A(n) é verdadeira para todo n. Na verdade, como sabemos do exemplo 1,

$$1 + 2 + 3 + 4 + ... + n \neq \frac{(n-1)(n+2)}{2}.$$

Exercício 3
Para cada uma das proposições, encontre os valores de $n \in \mathbf{N}$ para os quais a proposição é verdadeira, e também o menor valor de $n \in \mathbf{N}$ para o qual a proposição é falsa.
(a) $2^{n-1} \leq n^2$ (b) $n^2 + n + 1$ é um número primo.

É possível demonstrar por indução a validade dessas duas proposições? Justifique.

Exemplo 7 (Jakob Steiner – 1796-1863)

Mostre, usando indução, que o número máximo de regiões definidas por n retas no plano é $L_n = \frac{n(n+1)}{2} + 1$.

Solução

Para $n = 1$, o plano fica dividido em duas regiões, veja a Figura 3 a seguir.

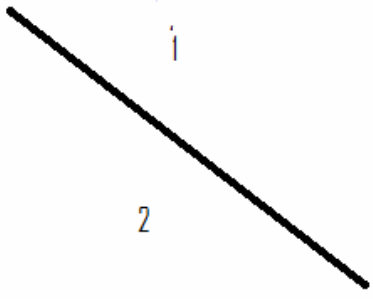

Figura 3 – Reta dividindo o plano em duas regiões

Desse modo, $L_1 = 2 = \frac{1.(1+1)}{2} + 1$. O que mostra que a afirmação é verdadeira para *n* = 1.

Traçando duas retas (não coincidentes), conforme a Figura 4, o plano fica dividido em 4 regiões. A expressão dada é verdadeira: $L_2 = 4 = \frac{2.(2+1)}{2} + 1$.

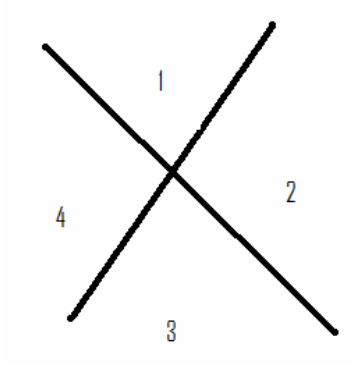

Figura 4 – Duas retas dividindo o plano em quatro regiões

Agora, observe que, traçando uma terceira reta, verificamos que esta divide no máximo três das quatro regiões já existentes, independentemente da posição das duas primeiras retas traçadas, veja a Figura 5 a seguir.

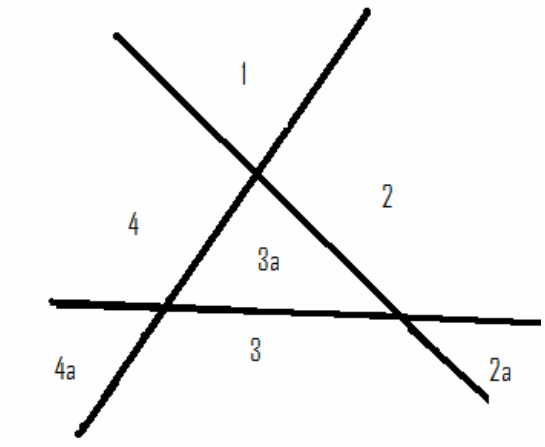

Figura 5 – Três retas dividindo o plano em sete regiões

Desse modo, com *n* = 3 retas, dividimos o plano em, no máximo, 7 regiões e a fórmula se verifica: $L_3 = 7 = \frac{3.(3+1)}{2} + 1$.

Observe que, $L_2 = L_1 + 2$, $L_3 = L_2 + 3$.

Agora, para $n \geq 1$, a n-ésima reta aumenta o número de regiões do plano de k se, e somente se, essa reta divide k das regiões já existentes. Por outro lado, a n-ésima reta intercepta k regiões já existente se ela intercepta as retas anteriores em $k - 1$ pontos. Mas, duas retas se interceptam em no máximo um ponto. Portanto, a n-ésima reta só pode interceptar as n - 1 retas anteriores em no máximo $n - 1$ pontos. Desse modo, como $k \leq n$, $L_n \leq L_{n-1} + n$.

Agora, desenhando a n-ésima reta de tal maneira que ela não seja paralela a nenhuma das outras n - 1 retas e não passe por nenhum dos pontos de interseção já existentes, temos que $L_n = L_{n-1} + n$. Essa igualdade foi verificada acima para $n = 2$ e $n = 3$. Observe que o passo da indução de n para $n + 1$ é dado por:
$L_{n+1} = L_n + (n + 1) =$

$$\left[\frac{n(n+1)}{2}+1\right]+(n+1)=\left[\frac{n(n+1)}{2}+(n+1)\right]+1=(n+1)\left[\frac{n}{2}+1\right]+1=\frac{(n+1)\left[(n+1)+1\right]}{2}+1$$

Portanto, o número máximo de regiões definidas por n retas no plano é $L_n = \frac{n(n+1)}{2}+1$, para todo número natural n.

Exemplo 8
Desenha-se n círculos num dado plano. Eles dividem o plano em regiões. Mostre que é possível pintar o plano com duas cores, azul e verde, de modo que regiões com fronteira comum tenham cores distintas.
Solução

Se $n = 1$, então, o plano fica dividido em duas regiões, uma externa ao círculo, que é pintada de azul, e a outra, região interna, pintada de verde, veja a Figura 6.

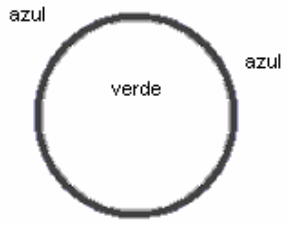

Figura 6 – O plano dividido por um círculo em duas regiões, pintadas com cores distintas.

Se $n = 2$, é fácil ver que podemos pintar o plano com duas cores, de modo que regiões com fronteira comum tenham cores distintas, veja a Figura 7 a seguir.

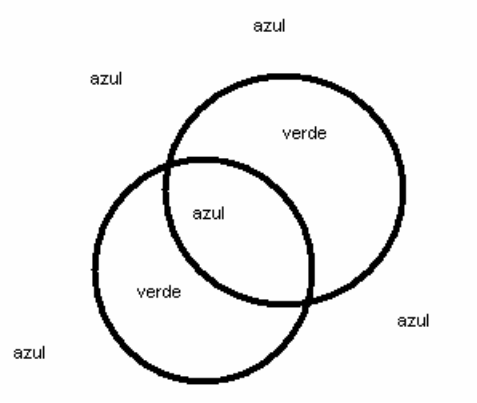

Figura 7 – O plano dividido em três regiões, pintadas de acordo com o problema.

Observe que, para fazer a pintura, no caso, de dois círculos, raciocinamos do seguinte modo: temporariamente, retiramos o segundo círculo e pintamos o plano de acordo com o caso de um único círculo. Agora, recolocamos o segundo círculo, deixando fixa a cor da região externa a ele e mudamos a cor da região comum aos dois círculos, de acordo com a Figura 7.

Vamos supor que, para o caso de *n,* seja possível pintar o plano com duas cores, de modo que regiões com fronteira comum tenham cores distintas. Para o caso de $n + 1$ círculos, raciocinamos como anteriormente. Isto é, removemos temporariamente o $(n + 1)$-ésimo mais um- círculo. O que sobra está nas condições da hipótese de indução, para o caso de *n* círculos. Agora, recolocamos o $(n + 1)$-ésimo círculo e mudamos alternadamente as cores das regiões internas a ele, deixando fixa a cor externa. Desse modo, as cores de regiões adjacentes ficam distintas. Portanto, para todo número natural *n,* é possível pintar o plano com duas cores, de modo que regiões com fronteira comum, determinadas pelos *n* círculos, tenham cores distintas.

Exercícios

(1) Mostre por indução que:

(a) $1.2 + 2.3 + 3.4 + 4.5 + ... + n(n+1) = \dfrac{n(n+1)(n+2)}{3}$

(b) $\dfrac{1}{1.2} + \dfrac{1}{2.3} + \dfrac{1}{3.4} + \dfrac{1}{4.5} + ... + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1}$

(2) Prove, usando indução, que o número de diagonais, d_n, de um polígono convexo de *n* lados é dado pela expressão: $d_n = \dfrac{n(n-3)}{2}$, $n \geq 4$.

(3) Prove, usando indução, que a soma, S_n, das medidas dos ângulos internos de um polígono convexo de *n* lados é dado pela expressão: $S_n = (n-2).180^o$, $n \geq 3$

(4) Considere uma Torre de Hanói dupla contendo $2n$ discos de *n* tamanhos diferentes, dois de cada tamanho. Como é usual, só podemos mover um disco de cada vez, sem colocar um maior sobre um menor.

Qual é o número mínimo de movimentos necessário para transferir a Torre de Hanói dupla, de um pino para outro, se discos de mesmo tamanho são indistinguíveis?

Sugestão – Inicialmente, pense em mover a torre dupla com $(n - 1)$ discos, depois, mover e inverter a ordem dos dois maiores discos e, finalmente, mover a torre dupla com $(n - 1)$ discos.

(5) Num país longínquo, a moeda local é o "cruzeiro". Nesse país, um banco tem uma quantidade ilimitada de cédulas de 3 e 5 cruzeiros.
Prove, por indução, que o banco pode pagar uma quantidade qualquer (inteira) de cruzeiros, maior do que sete.

(Sugestão: faça indução sobre o número de cruzeiros que o banco tem de pagar. Mostre que: se o banco pode pagar k, $k+1$, $k+2$ cruzeiros, então, o banco pode pagar $k+3$, $k+4$, $k+5$ cruzeiros).

(6) É permitido cortar uma folha de papel em 4 ou 6 pedaços. Prove que, aplicando essa regra, pode-se cortar uma folha de papel num número qualquer de pedaços maior do que 8.

(7) Prove, por indução, que todo número natural n pode ser representado como soma de diferentes potências de 2, que é a expansão de n na base 2.

Resumo

Nesta aula, estudamos o processo e o método de indução, que consiste em provar afirmações envolvendo números naturais. Para tanto, temos que provar que a afirmação é verdadeira para $n = 1$ e, supondo verdadeira para $n = k$, se pudermos provar que ela é verdadeira para $n = k + 1$, então, ela é verdadeira para todo número natural n.

Problemas Suplementares

Problema 1
Usando o Princípio da Indução, mostre que:

(a) $n^3 \geq 3n + 1$, para todo número inteiro maior do que ou igual a 2.
(b) $n^3 \geq 3n^2$, para todo número inteiro maior do que ou igual a 3.
(c) $3^n \geq n^3$, para todo número inteiro positivo.
(d) $|\text{sen. } n\text{os}| \leq n.|\text{sen. x}|$, para todo número real x e todo inteiro positivo n.

Problema 2
Prove, usando o Princípio da Indução, que todo polígono de n lados (convexo ou não) pode ser repartido em triângulos traçando diagonais.

Problema 3
Prove, usando o Princípio da Indução, que todo número inteiro positivo n pode ser escrito como uma soma do tipo $\pm 1^2 \pm 2^2 \pm 3^2 \pm .... \pm k^2$ **,** para algum inteiro positivo k e alguma escolha de sinais.

Problema 4

Cada vértice de um polígono convexo de n lados é pintado com uma cor. Para pintar todos os vértices usam-se no mínimo três cores, de tal maneira que vértices consecutivos têm cores distintas.

Prove, por indução, que podemos repartir o polígono em triângulo, usando diagonais que não se interceptam, de modo que os extremos das diagonais sejam pontos de cores distintas.

Problema 5

Numa ilha, cinco piratas dispõem de cem moedas de ouro para repartir entre si. Eles dividem o produto do saque da seguinte forma: o pirata mais velho propõe uma divisão e todos votam sim ou não. Se pelo menos a metade dos piratas vota sim, eles dividem as moedas da forma proposta. Caso contrário, matam o pirata mais velho e começam de novo. Então o pirata mais velho (sobrevivente) faz sua proposta de divisão e os outros votam de acordo com as mesmas regras, ou seja, repartem as moedas ou matam o mais velho, conforme o caso. O processo continua até que um plano seja aceito. Suponha que você é o pirata mais velho.

Que divisão você proporia, sabendo que todos os piratas são lógicos, gananciosos e querem continuar vivos?

Problema 6

O professor de Matemática escreve no quadro negro os números 1, 2, 2^2, 2^3, ..., 2^n e propõe o seguinte desafio. Um estudante pode apagar quaisquer dois dos números escritos e substituí-los pela diferença, tomada sempre maior do que ou igual a zero. Depois que este procedimento for repetido n vezes, restará um único número.

Que números podem restar no final dos procedimentos?

Referências

ANDREESCU, Titu; GELCA, Razvan. **Putnam and Beyond**. New York. Springer. 2007.

FERNANDES, Ângela Maria Vidigal et al. **Fundamentos de álgebra**. Belo Horizonte: Editora UFMG, 2005.

FOMIN, Dmitri; GENKIN, Sergey; ITENBERG, Ilia. **Mathematical circle**: Russian experience. Roadiland. American Mathematical Society, 1996.

GRAM, Ronald L.; KNUTH, Ronald E.; PATASHNIK, Oren. **Matémática concreta**: **fundamentos para a ciência da computação**. Rio de Janeiro: LTC, 1995.

HEFEZ, Abramo. **Elementos de aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2005.

POUNDSTONE, William. **Como mover o Monte Fuji?.** Rio de Janeiro. Ediouro. 2005.

STOROZHEV, Andrei. **International Mathematics Tournament of Towns 1997-2002. Book 5.** Canberra. AMT Publishing. 2006

WIKIPÉDIA. **Euclides**. Disponível em: <http://pt.wikipedia.org/wiki/Euclides>. Acesso em: 2 dez. 2008.

AULA 02 - Divisibilidade

Apresentação

Nesta aula, estudaremos o conceito de Divisibilidade no conjunto dos números inteiros, bem como suas propriedades básicas, que são importantes na Teoria dos Números.

Tente entender tudo que está sendo explicado na aula. Estude com caneta e papel ao lado. Seja paciente e procure ter certeza que você entendeu o que (e por que) está fazendo.

Objetivos

Com esta aula espera-se que você possa:

- Reconhecer quando um inteiro divide o outro;
- Usar as propriedades básicas da divisão de inteiros;
- Saber o que é um número primo.

PROPRIEDADES BÁSICAS DOS NÚMEROS INTEIROS

O conjunto dos números naturais **N** = {1, 2, 3, 4, 5, 6, ...} é o primeiro conjunto numérico que conhecemos, e é o cenário para os mais antigos e profundos problemas da Matemática.

Sabe-se que a soma (e o produto) de dois números naturais resulta em um número natural. Já a diferença entre dois números naturais nem sempre é um numero natural. Por exemplo, 5 – 8 = -3 e 4 – 4 = 0, que não são números naturais. Para suprir esta deficiência, amplia-se o conjunto dos números naturais para o conjunto dos números inteiros:

$$\mathbf{Z} = \{...-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, ...\},$$

que contém o conjunto **N,** o número zero e todos os inteiros negativos.

Os números naturais, 1, 2, 3, 4, 5, ... , são os **inteiros positivo**s. Simbolicamente, dizemos que um número inteiro *n* é positivo da seguinte maneira: $n > 0$ (leia-se: "*n* é maior do que zero" ou "*n* é positivo"). Os números....,-5, -4, -3, -2, -1 são os **inteiros negativos**. Simbolicamente, dizemos que um número inteiro *n* é negativo da seguinte maneira: $n < 0$ (leia-se: "*n* é menor do que zero" ou "*n* é negativo"). O número zero, "0", não é negativo nem positivo.

Como sabemos, os inteiros são munidos de duas operações: "+" (adição) e "x" (“““““ ““““ multiplicação, também representada por".").

Se *a*, *b* e *c* são números inteiros quaisquer, valem as seguintes propriedades para as duas operações de adição e multiplicação na tabela a seguir:

Tabela 1 – Propriedades básicas da adição e multiplicação de inteiros

Propriedade	**Adição**	**Multiplicação**
Associatividade	$a + (b + c) = (a + b) + c$	$a.(b.c) = (a.b).c$
Comutatividade	$a + b = b + a$	$a.b = b.a$
Identidade	$a + 0 = 0 + a = a$	$a.1 = 1.a = a$
Inverso	$a + (-a) = 0 = (-a) + a$	
Distributividade	$a.(b + c) = a.b + a.c$ $(a+b).c = a.c + b.c$	
Lei do Cancelamento	$a + c = b + c \Rightarrow a = b$	$a.c = b.c \Rightarrow a = b$, se $c \neq 0$

Se *a*, *b* e *c* são números inteiros quaisquer, dizemos que ***a* > *b*** *(*leia-se "a maior do que b") se, e somente se, a – b é um número inteiro positivo.

Propriedades dos Inteiros

Duas importantes propriedades dos inteiros são:

(a) **Tricotomia**
Se *a* e *b* são números inteiros quaisquer: o*u a* > *b ou b* > *a ou a* = *b.*
(Ou seja, dados dois inteiros *a* e *b,* uma, e somente uma, das possibilidades ocorre:

ou *a* é maior do que *b*
ou *b* é maior do *a*
ou *a* é igual a *b*)

(b) **Transitividade**
Se *a*, *b* e *c* são números inteiros quaisquer com *a* > *b* e *b* > *c*, então *a* > *c*

OS CONCEITOS DE DIVISIBILIDADE E NÚMERO PRIMO

Por volta de 300 a.c., Euclides reconheceu que a **divisibilidade** e os **números primos** são conceitos importantes para os números naturais. A seguir, vamos tratar destes dois conceitos.

Como podemos escrever 10 = 2 x 5, dizemos que 2 divide 10 (e que 5 divide 10). Ou seja, 2 é um divisor de 10 (e 5 é um divisor de 10) ou 2 é um fator de 10 (e 5 é um fator de 10).

Dizemos também que 10 é um múltiplo de 2 (e 10 é múltiplo de 5). Do mesmo modo, como 1001 = 11 x 91, dizemos que 11 divide 1001 (e que 91 divide 1001). Ou seja, 1001 é um **múltiplo de 11** (e 1001 **é múltiplo de 91**).

De uma maneira geral, se *a* e *b*, com *b* diferente de zero, são números inteiros e existe outro número inteiro *c* tal que *a = b.c*, dizemos que *b* divide *a (*e que *c* divide *a*). Neste caso, *b* (ou *c*) é dito ser um divisor de *a ou* um fator de *a*. Dizemos, também, que *a* é múltiplo de b e c.

Vejamos um exemplo, como 28 = 7 x 4, dizemos que 7 divide 28 (e que, também, 4 divide 28). Portanto, 7 e 4 são divisores de 28 ou fatores de 28 e 28 é múltiplo de 4 e de 7. De modo análogo, -4 é um divisor de 28 (ou um fator de 28), pois 28 = (-4) x (-7) e -3 é um divisor de -12, pois -12 = (-3) x 4.

Veja que os divisores de um número inteiro comparecem aos pares e quando *b.c = a,* então $b = \frac{a}{c} \quad e \quad c = \frac{a}{b}$.

Observe que a noção de divisibilidade é restrita ao fato de o divisor ser diferente de zero. Esta restrição provém do fato de que para todo inteiro *a*, tem-se *a.0 = 0,* o que implica $a = \frac{0}{0},$ para todo $a \in \mathbf{N}$, o que não faz sentido. Portanto, *0* **não pode ser divisor de qualquer inteiro.**

Observe que 7 **não divide** 12, pois não existe outro número inteiro *c* tal que 12 = 7 x c. Do mesmo modo, 20 **não divide** 30, pois não existe outro número inteiro *c* tal que 30 = 20 x c.

EXEMPLO 1
O conjunto S = {....., -12, -8, -4, 0, 4, 8, 12, 16, 20, ...} é a coleção de todos os múltiplos inteiros de 4, pois:

….., -12 = 4 .(-3); -8 = 4 .(-2); -4 = 4. (-1); 0 = 4.0; 4 = 4.1; 8 = 4.2; 12 = 4.3; 16 = 4.4; ……..

Deste modo, podemos descrever S como sendo a coleção de todos os inteiros da forma 4s, onde s é um número inteiro: S = {4s; s ∈ **Z**}.

Do modo análogo, U = {7, 14, 21, 28, 35, ...} é o conjunto dos múltiplos inteiros positivos de 7. Ou seja, U = {7m; m ∈ **Z**}

A seguir, vamos listar as propriedades básicas da divisão, apresentando suas respectivas provas.

Propriedades Básicas da Divisão

Se *a, b* e *c* são números inteiros, valem as seguintes propriedades:

(1) Se $a \neq 0$, então *a* divide *a* e *a* divide 0.
(2) Para qualquer *a*, 1 divide *a*.
(3) Se *a* divide *b* e *a* divide *c*, então *a* divide *bm* + *cn*, para todo *m* e *n* inteiros.
(4) Se *a* divide *b* e *b* divide *c*, então *a* divide *c*.
(5) Se *a* > 0 e *b* > 0, *a* divide *b* e *b* divide *a*, então *a = b.*
(6) Se *a* > 0 e *b* > 0, *a* divide *b*, então $a \leq b$.

Prova

(1) e (2). Estas propriedades seguem do fato que $a \cdot 1 = a$. e $a \cdot 0 = 0$

(3) Se a divide b, então existe x inteiro tal que $b = a.x$;

Se a divide c, então existe y inteiro tal que $c = a.y$.

Assim, $bm + cn = a.xm + a.yn = a.(xm + yn)$. Portanto, a é divisor de $bm + cn$.

(4) Se a divide b, então existe x inteiro tal que $b = a.x$. Se b divide c, então existe y inteiro tal que $c = b.y$. Assim, $c = b.y = (a.x).y = a.(x.y)$. Portanto, a divide c.

(5) Se a divide b, então existe x inteiro positivo tal que $b = a.x$. Se b divide a, então existe y inteiro positivo tal que $a = b.y$. Assim, $b = a.x = (by).x = b.(yx) \Rightarrow yx = 1 \Rightarrow y = 1$ e $x = 1$. Portanto, $a = b$.

(6) Se a divide b, então existe x inteiro positivo tal que $b = a.x$. Logo, $a \leq b$, pois como $a > 0$ e $x > 0$ tem-se $a \leq ax = b$.

É comum a seguinte notação para dizer que um inteiro a divide o inteiro b: $\boldsymbol{a \mid b}$.
Se *a não* divide b, notamos $a \nmid b$

EXEMPLO 2

Usando as propriedades básicas da divisão acima, concluir que:

$3 \mid (12m + 21n)$, quaisquer que sejam m, n inteiros.

Solução

É fácil ver que $3 \mid 12$ e $3 \mid 21$, pois $12 = 3.4$ e $21 = 3\ 7$.
Deste modo, $(12m + 21n) = (3.4.m + 3.7.n) = 3.(4m + 7n)$. Portanto, $3 \mid (12m + 21n)$.

EXERCÍCIO 1

(1) Verifique que 20 é divisível por cada um dos seguintes números: 1, 2, 4, 5, 10, 20.
(2) Verifique que 30 é múltiplo de cada um dos seguintes números: 1, 2, 3, 5, 6, 10, 15, 30.
3) Observe que $45 + 60 = 105$ e $105 - 60 = 45$.
(a) Explique porque qualquer divisor de 45 e 60 tem de ser um divisor de 105.
(b) Explique porque um divisor comum de 105 e 60 tem de ser um divisor comum de 45.
4) Verifique que 3 divide 228 e que 5 divide 725, mas 15 não divide 228 nem 725.

EXEMPLO 3

Verifique que a soma de três múltiplos de 5 é, também, um múltiplo de 5.

Solução

Observe que um múltiplo de 5 é da forma 5s, onde s é um número inteiro. Assim, se s, t e u são números inteiros, então 5s + 5t + 5u é a soma de três múltiplos de 5. Mas, 5s + 5t + 5u =

5(s + t + u), que é um múltiplo de 5, pois (s + t + u) é um inteiro. Portanto, a soma de três múltiplos de 5 é, também, um múltiplo de 5.

EXERCÍCIO 2

Explique porque a diferença entre dois múltiplos de 7 tem de ser um múltiplo de 7. E se em vez de 7 for 12? E se em vez de 12 for *n*?

Observe que, por mais que tentemos, não vamos conseguir escrever o número 7 como produto de dois números naturais $a \times b$, a menos que $a = 7$ e $b = 1$ ou $a = 1$ e $b = 7$. Isto quer dizer que: 7 só admite como divisores os números naturais 1 e 7. Neste caso, Euclides chamou 7 (e todos os números com essa propriedade) de **número primo.**

É fácil ver que 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97 são todos os números primos menores do que 100.

Uma pergunta: Existem quantos números primos?

Vamos demonstrar na Aula 5 que existem **infinitos números primos**. Você viu acima que existem 25 números primos menores do que 100.

De uma maneira geral, dizemos que um número natural *p* maior do que 1 é ***primo*** se *p* não pode ser escrito como produto de dois naturais entre 1 e *p*.

Observe que um número primo é, por definição, um número inteiro maior do que 1. Se um número natural não é primo, como, por exemplo, o número 10 = 2.5, dizemos que ele é um **número composto.** É fácil ver que 15 é um número composto, pois 15 = 3 . 5. Também o número 1071 é composto, pois 1071 = 3. 357. O número 2047 é composto, pois 2047 = 23 . 89.

É fácil ver que, proposições simples sobre os números naturais podem envolver métodos delicados de prova. De fato, para provar a proposição seguinte (aparentemente fácil):

(*) (EUCLIDES) *Se um número primo p divide o produto de dois número naturais a.b, então p divide a ou p divide b*

Euclides introduziu o conceito de **Máximo Divisor Comum (MDC)** e usou o **Algoritmo da Divisão** para expressar o MDC numa forma conveniente. Estes assuntos serão tratados nas aulas seguintes.

Para encerrar esta aula, vamos provar o seguinte resultado:

Dado um número inteiro positivo n, então o menor número natural maior do que 1 que divide n é um número primo.

Vamos supor que *p* é o menor número natural maior do que 1 que divide o número inteiro *n*. Assim, existe um número inteiro *c* tal que $n = p.c$. Se *p* não é primo, então $p = a.b$, onde $1 < a < p$ e $1 < b < p$. Isto é, $n = p.c = a.b.c$. Deste modo, *a* é um divisor de *n* e *a* é menor do que *p*. Contradição, pois *p* é o menor número natural maior do que 1 que divide *n.* Portanto, *p* é um número primo.

Exemplificando, o menor número natural maior do que 1 que divide 75 é 3, que é primo: 75 = 3.25. O menor número natural maior do que 1 que divide 87 é 3, que é primo: 87 = 3. 29. O menor número natural maior do que 1 que divide 100 é 2, que é primo: 100 = 2.50.

EXEMPLO 4
Qual é o menor número natural maior do que 1 que divide o número 91?
Solução

É fácil ver que 91 = 7 . 13. Portanto, o menor número natural maior do que 1 que divide 91 é 7 e, de fato, 7 é um número primo.

EXEMPLO 5
Se a e b são inteiros positivos e $ab = n$, então podemos concluir que $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.
Solução

Basta observar que: se $a \leq b$, então $n = ab \geq a.a = a^2$. Logo, $a \leq \sqrt{n}$. Por outro lado, se $a \geq b$, então $n = ab \geq b.b = b^2$. Logo, $b \leq \sqrt{n}$.

Concluímos que, o resultado acima indica que, um número inteiro n **não** é primo se ele tem um divisor positivo menor do que ou igual $\sqrt{n}$.

EXEMPLO 6
Diga, justificando, se o número 377 é primo.
Solução

Como $\sqrt{377} = 19{,}416.....$, pelo Exemplo 5, basta procurar um divisor para 377 dentre os inteiros primos de 1 até 19. É fácil ver que 13 divide 377 e, portanto, 377 não é primo.

EXERCÍCIO 3
Diga, justificando, se os números 187 e 211 são primos.

EXERCÍCIO 4
Identifique qual dos seguintes inteiros é primo:
(a) 91 (b) 191 (c) 791 (d) 771

EXEMPLO 6
A Teoria dos Números nos permite tratar do lado lúdico da Matemática.

Vivencie a seguinte brincadeira: **Como adivinhar a idade do amigo (a) ?**

Instruções:
Peça que ele (ela) escreva dois dígitos cuja diferença seja maior do que um.
Que entre os dois dígitos escreva um algarismo qualquer.

Peça que inverta a ordem dos algarismos do número obtido.
Peça que diminua o menor número obtido do maior.
Peça que inverta a ordem dos dígitos da diferença acima obtida.
Peça que some o último número obtido ao resto anterior.
Peça que some o número obtido à idade do amigo (a).
Peça para ele dizer qual o último resultado obtido.
Você então dirá a idade do amigo (a).
Qual é o truque?

Solução

Vamos imaginar que seu amigo escreveu os dígitos 7 e 2 e entre os dois colocou o número 4, formando o número 742. Seguindo as instruções, invertendo o número, obtém-se 247. Diminuindo o menor número do maior, tem-se: 742 – 247 = 495. Invertendo a ordem dos dígitos da diferença obtida, encontramos 594, que somado a 495 nos dá: 594 + 495 = 1089. Se a idade do amigo for, por exemplo, 17, você soma 1089 + 17 = 1106.

Qual é o truque?
O truque é o seguinte: qualquer que seja a escolha dos dígitos, antes de somar a idade do amigo, encontramos **sempre** o resultado 1089. Quando ele diz o resultado final, você subtrai 1089, obtendo a idade do amigo. Experimente com outros valores e comprove!

EXERCÍCIOS

1) Prove que: se $a \mid b$ e $a \mid c$, então: (i) $a \mid (b + c)$ (ii) $a \mid (b - c)$

2) Na tabela a seguir, identifique cada número primo, pintando de vermelho o quadradinho em que ele se encontra.

Tabela 2 – Os números naturais de 1 a 100.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

3) Responda as seguintes perguntas:

a) Qual é o menor inteiro positivo, maior do que 1, que divide 4189?
b) Qual é o menor inteiro positivo, maior do que 1 que divide 2627?

4) Dois amigos, A e B, se divertem com o seguinte jogo. O jogador A inicia o jogo escolhendo um dos inteiros de 1 a 8 (inclusive) e diz ao segundo jogador, que escolhe

um número qualquer de 1 a 8 e soma esse número com o que A escolheu, falando o resultado ao primeiro jogador, que, por sua vez, o soma a qualquer número escolhido de 1 a 8, e assim eles vão jogando, alternadamente. O jogador que primeiro obtiver o número 46 **perde** o jogo.
Quem vence: A ou B? Qual é a estratégia para vencer?

(Sugestão: O vencedor na sua última jogada, para ter certeza que vence o jogo, deve atingir que número? Qual é a primeira jogada do vencedor?)

5) Encontre três divisores inteiros positivos de 30.

6) Diga, justificando, se 39 é um número primo ou composto.

7) Dê exemplo de quatro pares de números naturais (p, q), onde p e q são primos, com $p > q$ e $p - q = 2$.

8) Escreve-se no quadro-negro os números inteiros de 1 a 15. Você escolhe quaisquer dois destes números, apaga-os, e junta à lista a soma deles. Depois de quatorze operações deste tipo, resta somente um número sobre o quadro-negro.
Em cada operação realizada, é possível fazer escolhas de modo que o número final seja 105?

(Sugestão: Quanto é a soma: 1 + 2 + 3 + 4 + ... + 15?)

9) Dois amigos, A e B, se divertem com o seguinte jogo. O jogador A inicia o jogo escolhendo um dos inteiros de 1 a 8 (inclusive) e diz ao segundo jogador, que escolhe um número qualquer de 1 a 8 e soma esse número com o que A escolheu, falando o resultado ao primeiro jogador, que, por sua vez, o soma a qualquer número escolhido de 1 a 8, e assim eles vão jogando, alternadamente, até que um deles obtenha o número 46, **vencendo** o jogo.
a) Quem vence o jogo: A ou B? b) Qual é a estratégia para vencer?

(Sugestão: O vencedor na sua penúltima jogada, para ter certeza que vence o jogo, deve atingir que número? Qual é a primeira jogada do vencedor?)

RESUMO

Nesta aula estudamos os conceitos de divisibilidade e suas propriedades e o de número primo, indispensáveis e fundamentais no estudo da Teoria dos Números.

Problemas Suplementares

Problema 1
Encontre todos os números inteiros positivos n para os quais os números $n^{10} + 1$ sejam divisíveis por $n + 1$.

Problema 2
Mostre que: para todo inteiro positivo n, o número $n^4 + 64$ é um número composto.

Problema 3
Seja p um número primo maior do que ou igual a 5. Mostre que $p^2 + 2$ é um número composto.

Problema 4
Encontre o menor número inteiro positivo n para o qual os números:

$$n,\ n+1,\ n+2,\ n+3,\ n+4,\ n+5,\ n+6,$$

sejam todos compostos.

Problema 6
Mostre que não existe polinômio com coeficientes inteiros, P(x), satisfazendo as igualdades: P(7) = 5 e P(15) = 9.

Referências

ANDREESCU, Titu; GELCA, Razvan. **Putnam and Beyond**. New York. Springer. 2007.

Burton, David M. – **Elementary Number Theory**. The McGraw-Hill Companies, Inc. New York. USA. 1998

Coutinho, S. C. – **Números Inteiros e Criptografia RSA**. Instituto de Matemática Pura e Aplicada – IMPA & Sociedade Brasileira de Matemática – SBM. Rio de Janeiro. Brasil. 1997

Hefez, Abramo – **Elementos de Aritmética**. Sociedade Brasileira de Matemática. Rio de Janeiro. Brasil. 2005

Perelmán, Ya I. – **Problemas y Experimentos Recreativos**. Editorial MIR. Moscú. URSS. 1975

Aula 3 – O algoritmo da divisão

Apresentação

Nesta aula, estudaremos o Algoritmo da Divisão, proposto por Euclides, e seus usos nas questões de divisibilidade dos números inteiros.

O que nesta aula você vai aprender não são somente fatos, imaginamos poder trilhar, juntos, caminhos amigáveis para você aprender a Teoria dos Números. Para obter sucesso, a partir desta aula, você tem que ler e compreender o conteúdo. Leia devagar, gastando alguns minutos numa única linha, se isso for necessário. Não se impaciente. Avance quando você se achar preparado.

Objetivos

- Fazer uso do Algoritmo da Divisão na solução de problemas envolvendo números inteiros.

- Compreender que o uso do Algoritmo da Divisão permite expressar um número inteiro de forma unívoca a partir da sua divisão por outro número.

Noções básicas

Observe que o inteiro 5 não divide o inteiro 42 e que 7 não divide 12. Por outro lado, podemos escrever $42 = 8.5 + 2$ e $12 = 1.7 + 5$. É fácil criar vários exemplos de dois números inteiros onde um número não divide outro. Assim, concluímos que a divisão é bastante restritiva no conjunto dos números inteiros.

Existe um processo de divisão de um número natural qualquer por outro, que amplia o conceito de divisibilidade e pelo qual se determina o **quociente** e o **resto da divisão**, sendo eles determinados unicamente. Esse processo é conhecido como **Algoritmo da Divisão** (apresentado por Euclides), e se estende de modo natural para o conjunto de todos os inteiros, com a restrição do divisor ser diferente de zero (ou divisor positivo, para facilitar).

O Algoritmo da Divisão

Sabemos que 5 não divide 38, mas, no entanto, podemos escrever $38 = 7.5 + 3$. Nesse caso, 7 é o **quociente** e 3 é o **resto da divisão** de 38 por 5. Outro exemplo é $42 = 5.8 + 2$, nesse caso, 5 é o **quociente** e 2 é o **resto da divisão** de 42 por 8. Outro exemplo, $-26 = (-7).4 + 2$, nesse caso, -7 é o **quociente** e 2 é o **resto da divisão** de -26 por 4. Agora, observe que, como 5 divide 35, podemos escrever $35 = 7.5 + 0$; nesse caso, 7 é o **quociente** e 0 é o **resto da divisão** de 35 por 5. É nesse sentido que dizemos que o Algoritmo de Euclides amplia o conceito de divisibilidade. De uma maneira geral temos:

Algoritmo da Divisão

Dados dois números inteiros n e d, com d > 0, existem dois números inteiros q e r tais que nb = q.d + r, com 0 ≤ r < d. Além disso, os números q e r são únicos, para cada par de números n e d dados.

Antes de demonstrar o Algoritmo da Divisão, de Euclides, vamos apresentar uma propriedade muito interessante do conjunto dos números inteiros, que utilizaremos na demonstração do Algoritmo de Euclides. Trata-se do **Princípio do Menor Inteiro** (também chamado de **Princípio da Boa Ordenação** ou **Princípio da Boa Ordem)**.

Princípio do Menor Inteiro

Todo subconjunto não nulo de números inteiros positivos possui um menor elemento.

O Princípio do Menor Inteiro é aceito sem demonstração porque ele é intuitivo e se comprova facilmente com qualquer exemplo. Além disso, pode-se mostrar que o Princípio do Menor Inteiro é equivalente ao Princípio da Indução. Se A = {5, 7, 9, ..., 99}, então, o menor elemento de A é o 5. Se B = {x ∈ **Z** | x = n^2 + 1, onde *n* é um inteiro qualquer}, então o menor elemento de B é 1 (que ocorre quando *n = 0).* Você pode criar vários outros exemplos para verificar a veracidade do Princípio do Menor Inteiro.

Agora, vamos apresentar duas demonstrações do Algoritmo da Divisão. É interessante observar que a demonstração do Algoritmo da Divisão tem duas partes distintas: uma é a existência e a outra a unicidade.

Demonstração 1

(i) Existência

a) Suponha inicialmente que *n* é um número natural.
Vamos usar o Princípio da Indução, estudado na aula 1 – Noções sobre o processo e o método de indução – fazendo indução sobre *n*.
Para *n* = 1, tem-se *q* = 1 e *r* = 0 no caso *d* = 1, pois 1 = 1.1+ 0. No caso *d* > 1, tem-se *q* = 0 e *r* = 1, uma vez que 1 = 0.*d* + 1.
Suponhamos o algoritmo válido para *n* = *k*, isto é, *k* = *q.d* + *r,* com 0 ≤ *r* < *d*.
Desse modo, *k* + 1 = *q.d* + *r* + 1. Como 0 ≤ *r* ≤ *d* – 1, analisemos os casos 0 ≤ r ≤ *d* – 2 e *r* = *d* – 1 separadamente.
Se for *r* = *d* – 1, então, *r* + 1 = *d*, o que dá *k* + 1 = *q.d* + *d* = (*q* + 1).*d*. Logo, *k* + 1 dividido por *d* tem *q* + 1 como quociente e resto zero.
Agora, se 0 ≤ r ≤ *d* – 2, então, 1 ≤ r + 1 ≤ d – 1. Desse modo, fica
k + 1 = *q.d* + *(r* + 1), onde 1 ≤ *(r* + 1) ≤ *d* – 1. Portanto, o algoritmo também é válido para *n* = *k* + 1. Pelo Princípio da Indução, o algoritmo é válido para todo número natural *n*.

b) Ora, de *n* = *q.d* + *r,* com 0 ≤ *r* < *d*, segue que:
Se *r* = 0, temos: -*n* = (-*q*)*d* + 0. Caso contrário, - *n* = (-*q*).*d* – *r* = (-*q*).*d* – *d* + *d* – *r* = (-*q* – 1).*d* + (*d* – *r*). Como 0 ≤ *r* < *d*, então, 0 < *d* – *r* < *d*. Desse modo, o algoritmo é válido para todo inteiro negativo.

c) Para $n = 0$, tem-se zero como quociente e resto, pois $0 = 0.d + 0$.

Conclusão: de a), b) e c), segue que o Algoritmo da Divisão é válido para todo inteiro *n,* o que conclui a prova.

(ii) Unicidade

Resta mostrar que os números inteiros q e r são únicos, para cada par de números inteiros *n, d* dado. Vamos supor que existam dois inteiros u e v, tais que $n = q.d + r$ e $n = u.d + v$, com $0 \leq r < d$ e $0 \leq v < d$. Vamos supor que $u < q$. Logo, $u + 1 \leq q$, pois u e q são inteiros. Podemos concluir que:

$r = n - q.d \leq n - (u + 1).d = n - u.d - d = v - d < 0$. Contradição, pois $r \geq 0$.

O mesmo raciocínio pode ser usado para o caso em que $u > q$, obtendo uma contradição.
Pela propriedade da Tricotomia (vista na aula 1), só resta $u = q$. Portanto, temos
$n = q.d + r$ e $n = q.d + v$, o que implica $r = v$. Logo, a unicidade está provada.

Demonstração 2

(i) Existência

Suponhamos por absurdo que o Algoritmo da Divisão não é válido. Isto é, existe $n \in \mathbf{Z}$ e $d \in \mathbf{N}$ tais que, para todo $f \in \mathbf{Z}$, se $r = n - f.d$, então, $r < 0$ ou $r \geq d$. Essa hipótese nos remete a considerar o conjunto $S = \{n - fd \mid n - fd \geq 0\}$.
Mostremos que S não é o conjunto vazio.
De fato, se $n \geq 0$, tomando $f = -1$, fica $n - f.d = n + d \geq d$. Isso nos diz que $n + d \in S$.
Se, por outro lado, $n < 0$, tomando $f = n - 1$, temos que $n - f.d = n - (n - 1).d = n - nd + d > d$, pois $n - nd > 0$. Logo, $n - (n - 1).d \in S$.
Sendo $S \neq \varnothing$ e limitado inferiormente por d, pelo Princípio do Menor Inteiro, S possui um menor elemento; $n - q_o .d$.
Por outro lado,
$n - (q_o + 1) .d = n - q_o .d - d < n - q_o .d$.
Como $n - q_o .d$ é o menor elemento de S, então, $n - (q_o + 1) .d$ não pertence a S. Pela hipótese inicial, dever ser $n - (q_o + 1) .d < 0$. Isso implica que $n - q_o .d < d$, o que é uma contradição, pois $n - q_o .d \geq d$.
Portanto, a hipótese inicial é falsa, o que acarreta que o Algoritmo da Divisão é válido para todo número $n \in \mathbf{Z}$ e todo $d \in \mathbf{N}$.

(ii) Unicidade

Veja a demonstração anterior.

No Algoritmo da Divisão, b = q.a + r, a é dito divisor, b é o dividendo, q é o quociente e r é o resto. Assim, podemos escrever: dividendo = quociente $\times$ divisor + resto. Certamente, você já foi apresentado a esse algoritmo com essa versão simplificada.

Uma das mais importantes conseqüências do Algoritmo da Divisão é que qualquer inteiro m ou é divisível por a (sendo a inteiro maior do que 1) ou deixa resto 1 ou 2 ou 3 ou... ou $a - 1$ na divisão por a. Logo, no caso em que $a = 2$, conclui-se que todo inteiro ou é da forma $2q$ ou da forma $2q + 1$, sendo q um número inteiro, pois os possíveis restos na divisão por 2 são: 0 ou 1.

Quando um inteiro b é da forma $2q$, com q um número inteiro (ou seja, deixa resto zero na divisão por 2), dizemos que b é um **número par**. Quando um inteiro b é da forma $2q + 1$, com q um número inteiro (ou seja, deixa resto 1 na divisão por 2), dizemos que b é um **número ímpar.**

Usando a divisão por 3, podemos concluir que todo número inteiro m é da forma 3q ou 3q + 1 ou 3q + 2 (ou seja, ou deixa resto zero ou deixa resto 1 ou deixa resto 2, quando dividido por 3).

Exemplo 1
O quadrado de qualquer inteiro ou é da forma $4q$ ou $4q + 1$, onde q é um inteiro.
Solução

Dado um inteiro b qualquer, temos que: ou b é par ou b é ímpar. Logo, ou $b = 2k$ ou b = $2k + 1$, onde k é um inteiro. Portanto, ou $b^2 = 4k^2 = 4q$, onde $q = k^2$,

ou $b^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1 =$

$= 4q + 1$, onde $q = k^2 + k \in \mathbf{Z}$.

Portanto, o quadrado de qualquer inteiro é da forma $4q$ ou $4q + 1$, onde q é um inteiro.

Exemplo 2
A soma dos quadrados de dois inteiros é da forma $4q$ ou $4q + 1$ ou $4q + 2$, onde q é um inteiro.
Solução

Pelo exemplo 1, dados dois inteiros a e b, seus quadrados, a^2 e b^2, só podem ser da forma $4q$ ou $4q + 1$, onde q é um inteiro. Portanto, a soma dos quadrados, $a^2 + b^2$, só pode ser da forma:
$4m + 4n = 4q$, *com* $m + n = q$, ou
$4m + (4n + 1) = 4q + 1$, com $m + n = q$ ou
$(4m + 1) + (4n + 1) = 4q + 2$, com $m + n = q$.

Exercício 1

Se n é um inteiro positivo qualquer, verifique que o número $\frac{n(n+1)}{2}$ é um inteiro.

Exemplo 3
Prove que nenhum inteiro da forma $4q + 3$, onde q é um inteiro, pode ser escrito como soma de dois quadrados.
Solução

É uma conseqüência imediata do exemplo 2, pois a soma dos quadrados de dois inteiros tem que ser da forma $4q$ ou $4q + 1$ ou $4q + 2$, onde q é um inteiro.

Exemplo 4
Nenhum número da lista abaixo é um quadrado perfeito, isto é, um quadrado de um número inteiro:

11, 111, 1111, 11111, 111111, 1111111, ...

Solução

Basta observar que todo número da lista é da forma $4q + 3$, com $q \in \mathbf{Z}$. Veja, por exemplo, que:

$11 = 4.2 + 3;$
$111 = 4.27 + 3;$
$1111 = 4.277 + 3$ etc.

Mas, de acordo com o exemplo 1, o quadrado de qualquer número inteiro é da forma $4q$ ou $4q + 1$, onde q é um inteiro. Logo, nenhum número da lista dada é um quadrado perfeito.

Exercício 2

1) Encontre o quociente e o resto na divisão de:
(a) 227 por 143 (b) 1479 por 272 (c) 2378 por 1769

2) Quantos inteiros entre 100 e 200 deixam resto 5 quando divididos por 7?

Observe que no enunciado do Algoritmo da Divisão não é exigido que o dividendo b seja um número positivo, mas que apenas o divisor seja. Por exemplo, $b = -123$ e $a = 15$, então, $q = -9$ e $r = 12$. Ou seja, $-123 = (-9).15 + 12$.

Exemplo 5

Os números inteiros positivos são arrumados em 7 colunas conforme a disposição a seguir.

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
.....	.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....	.....

Qual é a linha e coluna em que se encontra o número 1500?

Solução

Observe na disposição anterior que, na primeira coluna, contando da esquerda para a direita, estão colocados todos os números inteiros positivos que deixam resto 1 quando divididos por 7. Na segunda coluna, estão os números inteiros positivos que deixam resto 2 quando divididos por 7, e, assim por diante, até a sétima coluna, onde estão os números inteiros positivos que deixam resto zero quando divididos por 7. Agora, para identificar a coluna em que se encontra o número 1500, basta calcular o resto da divisão de 1500 por 7. Como $1500 = 214. 7 + 2$, temos que 1500 encontra-se na segunda coluna, contado da esquerda para a direita

Exercícios

1) Liste todos os inteiros entre 0 e 50 que podem ser expressos na forma $8n$ para algum inteiro n.

2) Liste todos os inteiros entre 0 e 50 que podem ser expressos na forma $8n + 3$ para algum inteiro n.

3) Liste todos inteiros entre 0 e 50 que podem ser escritos na forma 8n + 7 para algum inteiro n.

4) Ache o menor múltiplo positivo de 5 que deixa resto 2 quando dividido por 3 e 4.

5) Use o Algoritmo da Divisão para concluir que:
(a) O cubo de qualquer inteiro tem uma das formas seguintes: $9q$, $9q + 1$ ou $9q + 8$.
(b) Nenhum número da forma $3q^2 - 1$ é um quadrado perfeito.

6) Dado um inteiro qualquer n, conclua, usando o Algoritmo da Divisão, que o número $\frac{n(n+1)(2n+1)}{6}$ é um inteiro.

7) Encontre o quociente e o resto na divisão de:
(a) 2^{2009} por 3 (b) 15^{2008} por 7 (c) 2008^{2009} por 1601

8) Quantos inteiros entre 100 e 200 deixam resto 5 quando divididos por 7?

9) Quantos inteiros entre 0 e 200 deixam resto 4 quando divididos por 6?

10) Encontre o maior número inteiro de três dígitos que deixa resto 5 quando dividido por 8.

11) Encontre o menor número natural múltiplo de 7 que deixa resto 1 na divisão por 3 e 4.

12) Arrumam-se os números inteiros positivos ímpares 1, 3, 5, 7, 9, 11, ..., em cinco colunas, conforme a disposição a seguir.

	1	3	5	7
15	13	11	9	
	17	19	21	23
31	29	27	25	
	33	35	37	39
47	45	43	41	
	49	51	53	55
63	61	59	57	
.....	.....	.....	.....	.....
.....	.....	.....	.....	.....

Contando da esquerda para a direita, qual é a coluna em que se encontra o número 2009?

Sugestão – Observe que todos os números positivos ímpares entre 0 e 8 estão na primeira fila e, de um modo geral, todos os números inteiros positivos ímpares entre $8(n - 1)$ e $8n$ estão na

n-ésima fila. Agora, verifique se o número 2009 está numa fila par ou ímpar e se os números crescem ou decrescem naquela fila.

13) Quais são os números que, quando divididos por 7, deixam resto igual:
(a) à metade do quociente? (b) ao quociente?
(c) ao dobro do quociente? (d) ao triplo do quociente?

14) O resto da divisão de um número inteiro n por 15 é 5. Qual é o resto da divisão de n por 7?

15) Como adivinhar o dia e mês do seu nascimento ?
Escreva numa folha de papel o dia do mês em que você nasceu e faça as operações seguintes:
duplique o número escrito;
multiplique por 10 o número obtido;
some 73 ao produto;
multiplique por 5 a soma;
Ao total adicione, o número de ordem do mês em que você nasceu (por exemplo, se você nasceu em agosto esse número é 8); diga o resultado final de todas as operações.
Com esse número posso dizer exatamente o dia e o mês em que você nasceu.
Como posso fazer isso?

Resumo
Nesta aula, estudamos o importante Algoritmo da Divisão e vimos como ele é indispensável no estudo da divisibilidade dos números inteiros.

Problemas Suplementares

Problema 1
Três escolas pediram a uma mesma livraria as respectivas quantidades de certo livro didático: 90, 126 1 198. A livraria pretende entregar esses livros, numa única viagem, por meio de pacotes iguais, isto é, todos com a mesma quantidade de livros.
Qual é o número mínimo de pacotes que essa livraria conseguirá formar para atender os tais pedidos?

Problema 2
Num luminoso de rua, uma lâmpada amarela pisca de 6 em 6 segundos e uma lâmpada vermelha pisca de 9 em 9 segundos. Se às 8 horas da noite elas piscam juntas, desse instante até as 11 horas da mesma noite, quantas vezes elas piscam simultaneamente?

Problema 3
Sabe-se que m, n e p são três números inteiros positivos, tais que: $m < n$ e $m.n + p.n = 58$. Descubra que número é o p.

Problema 4

Joãozinho exagerou na bagunça na sala de aula e o professor, como forma de castigo, mandou que ele resolvesse o seguinte problema: “Encontre um número natural, maior do que 100, cujo quadrado ao ser dividido por 3 deixa resto 2”.
Qual foi a resposta de Joãozinho?

Problema 5
Considere todos os números naturais do conjunto {500, 501, 502, 503, ..., 1999}.
Qual é a soma de todos os restos das divisões, por 5, de todos os números do conjunto dado?

Problema 6
No subconjunto de números inteiros S = {1881, 1882, 1883, ..., 2009}, quantos são os números divisíveis por 117?

Problema 7
Mostre que, para quaisquer que sejam os inteiros m e n, o produto $(36a + b).(a + 36b)$ não pode ser uma potência de 2.

Referências

BURTON, David M. **Elementary number theory**. New York: McGraw-Hill, 1998.

COUTINHO, S. C. **Números inteiros e criptografia RSA**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada – IMPA/ Sociedade Brasileira de Matemática – SBM, 1997.

HEFEZ, Abramo. **Elementos de aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2005.

NERY, Chico. **Para gostar de Matemática**, Vols 1 e 2. Ribeirão Preto. Editora São Francisco. 2008

PERELMÁN, Ya I. **Problemas y experimentos recreativos**. Moscú: Editorial MIR, 1975.

Aula 4 - O teorema fundamental da aritmética

Apresentação

Na aula 2 (Divisibilidade), você teve o primeiro contato com os números primos. Eles constituem um dos objetos mais fundamentais da Matemática. O aspecto de indivisibilidade que carrega consigo cada número primo, tem despertado o interesse e a admiração dos matemáticos ao longo dos séculos. A importância dos primos se deve à capacidade que eles têm de gerar todos os números inteiros, veremos adiante quando abordarmos o Teorema Fundamental da Aritmética. Tal importância tem motivado o estudo dos números primos desde a antiguidade grega até os nossos dias.

Tente entender tudo que está sendo explicado na aula. Estude com caneta e papel ao lado. Leia com atenção. Se for preciso, leia várias vezes uma linha ou um parágrafo. Seja paciente e procure ter certeza que você entendeu o que (e por que) está fazendo.

É importante que tente resolver cada um dos problemas que aparece no final da aula, na auto-avaliação, pois será um teste para avaliar seu entendimento acerca do conteúdo apresentado.

Objetivos

- Decompor um número inteiro positivo em seus fatores primos.
- Usar a decomposição de dois números inteiros positivos em fatores primos para encontrar o Máximo Divisor Comum e o Mínimo Múltiplo Comum desses dois números.
- Encontrar o número de divisores de um número inteiro positivo.

O papel fundamental dos números primos

Desde a Grécia antiga, os químicos se esforçaram para identificar os elementos básicos da natureza. Tal esforço culminou com a elaboração da tabela periódica de Dimitri Mendeleev (1834 -1907), professor da Universidade de São Petersburgo, na Rússia. Cada uma das moléculas do mundo físico pode ser decomposta por átomos da tabela periódica de elementos químicos. Para os matemáticos, os números primos são os elementos de nossa tabela periódica. Mas, apesar do sucesso que os gregos antigos tiveram na identificação de blocos de números que permitem um amplo domínio da aritmética, os matemáticos têm dificuldade de entender a tabela dos números primos.

O matemático que primeiro construiu uma tabela de primos foi Eratóstenes, que foi diretor da biblioteca de Alexandria no século III a. C.

A lista de matemáticos que se esforçaram para entender a tabela dos números primos é imensa, contando com nomes como Euclides, Fibonacci, Gauss, Euler, Goldbach, Riemann, Fourier, Jacobi, Legendre, Cauchy, Hilbert, Hardy, Littlewood, Ramanujan, Minkowski, Landau etc. Até os dias de hoje ainda se procura entender a tabela dos primos.

Em 1970, , três pesquisadores que trabalhavam no Massachussets Institute of Tecnology – MIT, nos Estados Unidos, Ron Rivest, Adi Shamir e Leonard Adleman, explorando os

trabalhos de Pierre de Fermat, feitos no século XVII, descobriram um modo de usar os números primos para proteger nossos cartões de créditos, quando fazemos compras pela Internet. Sem o poder dos números primos, esse tipo de comércio jamais poderia existir.

Os três pesquisadores citados usaram um processo para manter o número de nossos cartões de crédito em segurança, usando números primos com 100 dígitos. O sistema inventado se chama RSA, sendo R a primeira letra do segundo nome do primeiro cientista, S a primeira letra do segundo nome do segundo cientista e A a primeira letra do segundo nome do terceiro. Hoje em dia, para aumentar a segurança, já se usa números primos com 600 dígitos.

Eratóstenes, astrônomo e matemático grego que foi diretor da biblioteca de Alexandria na época de Ptolomeu III, inventou uma técnica para achar todos os primos menores do que ou iguais a um dado número n, que ficou conhecida como **Crivo de Eratóstenes**. A técnica consistia em listar todos os números de 2 até n; em seguida, riscar todos os múltiplos de 2, maiores do que 2; logo após, riscar todos os múltiplos de 3, maiores do que 3; depois, riscar todos os múltiplos de 5, maiores do que 5, e assim por diante. Eratóstenes sabia que um dos fatores primos de um número composto era menor do que ou igual à raiz quadrada do número. Assim, ele continuaria o processo até que o maior número primo menor do que ou igual a $\sqrt{n}$ fosse atingido. Nessa altura, todos os números compostos de 2 até n já teriam sido riscados, restando somente os números primos de 2 até n.

Eratóstenes também foi atleta, poeta, filósofo e historiador. Como atleta, fez sucesso nos III Jogos Olímpicos, da Grécia antiga.

Agora, vamos responder completamente à pergunta feita na aula 2:

Existem quantos números primos?

Conforme afirmamos antes, Euclides, em sua obra *Os Elementos*, demonstrou o seguinte:

Teorema 1
Existem infinitos números primos.
Demonstração 1

Antes de dar a demonstração de Euclides, vamos entender a sua idéia. O que Euclides fez foi construir um número que não pudesse ser gerado por qualquer lista finita de primos que lhe fosse apresentada. Por exemplo, considere a lista dos seis primeiros primos: 2, 3, 5, 7, 11 e 13. Euclides multiplicou-os, obtendo o número 2 x 3 x 5 x 7 x 11x 13 = 30030, que é um múltiplo dos seis primeiros primos. A seguir, usando sua genialidade, somou 1 ao produto, obtendo 30031, que não é divisível por nenhum dos cinco primos da lista, pois a divisão de 30031 por qualquer um dos cinco primos deixa resto 1. Euclides sabia que o número criado poderia não ser primo, mas se não fosse, deveria ser divisível por um primo que não estava na lista dada. Assim, Euclides disse que qualquer que fosse a lista finita dos primos, era possível criar um número que só poderia ser formado a partir de primos que não estavam na lista dada. O número do exemplo, 2 x 3 x 5 x 7 x 11x 13 + 1 = 30031 = 59 x 509, portanto, não é primo. Agora que você já entendeu a idéia de Euclides, vamos fazer a demonstração do Teorema 1.

Vamos imaginar que a quantidade de primos não seja infinita. Significa que, ao listar todos os primos, essa lista terminaria em algum primo, ou seja, teria um primeiro primo, um segundo, ..., e um último. Assim, vamos supor que existem somente n números primos:

$$p_1, p_2, p_3, p_4, ..., p_n$$

de maneira tal que eles estejam ordenados em ordem crescente: $p_1 < p_2 < p_3 < p_4 < ..... < p_n$. Isso seria o mesmo que colocar $2 < 3 < 5 < 7 < 11 < 13 < 17 < 23 < ..... < p_n$, sendo p_n o maior de todos. Agora, vamos tomar o seguinte número, M, construído a partir de todos os n primos:

$$M = p_1.p_2.p_3.p_4.....p_n + 1.$$

Observe que M é um inteiro positivo maior do que qualquer um dos primos. De fato, $M > 2p_n + 1$, pois 2 é o menor número primo. Logo, M é maior do que p_n, o maior de todos os primos e, portanto, maior do que todos os primos $p_1, p_2, p_3, p_4, ..., p_n$. Logo, por hipótese, M não é primo. Assim, M é divisível por algum primo. Mas, esse primo deveria ser um dos primos $p_1, p_2, p_3, p_4, ..., p_n$. Escolha um desses, digamos p_i, para ser o divisor de M. Nesse caso, teríamos número $M - p_1.p_2.p_3.p_4...p_i....p_n = 1$ e como p_i divide M e p_i divide $p_1.p_2.p_3.p_4...p_i....p_n$, segue que p_i divide 1, o que implica que $p_i = 1$, o que é uma contradição.

Demonstração 2
Suponha que a quantidade dos primos seja finita e $p_1 = 2 < p_2 = 3 < p_3 = 5 < p_4 = 7 < .... < p_n$ os primos. Considere m o menor número inteiro positivo maior do que p_n. Agora, considere o número inteiro positivo $m! + 1$. Como $m! + 1 > p_n$, ele não pode ser primo. Logo, $m! + 1$ é divisível por um dos primos já enumerados anteriormente. Por outro lado, o produto 1.2.3.....$m = m!$ tem esse primo como um de seus fatores. Logo, esse primo divide 1, o que constitui uma contradição.

Exemplo 1
Diga, justificando, se o número $M = 2.3.5.7 + 1$ é primo.
Solução

$M = 2.3.5.7 + 1 = 211$. Você viu, no exemplo 5 da aula 2 (Divisibilidade) que se um número inteiro positivo n não é primo, então, n possui um divisor menor do que ou igual a $\sqrt{n}$.
Como $\sqrt{M} = \sqrt{211} = 14{,}525839...$, basta procurar um divisor primo menor do que ou igual a 13. Como 2, 3, 5, 7, 11 e 13 não dividem M, então, M é um número primo.

Exercício 1
Qual é o maior divisor primo do número inteiro $1 + 2 + 3 + 4 + ... + 50$?

O teorema fundamental da aritmética

O Teorema Fundamental da Aritmética coloca em evidência o papel dos números primos na estrutura dos inteiros. Ele nos assegura que um número pode ser expresso como um produto de números primos de modo único, a menos da ordem desses fatores primos.

Considere o número 90. Esse número só pode ser expresso como produto de primos usando somente os primos 2, 3 e 5, a menos da ordem. De fato, podemos escrever:

90 = 2 x 3 x 3 x 5 = 3 x 3 x 2 x 5 = 2 x 5 x 3 x 3 = 2 x3 x 5 x 3 = = 5 x 3 x 2 x 3 = 3 x 2 x 3 x 5 = 3 x 2 x 5 x3 = 3 x 5 x 2 x 3 etc. Resumidamente, $90 = 2 \times 3^2 \times 5$.

De modo análogo, considere o número 24. Ele só pode ser expresso como produto de primos usando somente o 2 e o 3, a menos da ordem:

24 = 2 x 2 x 2 x 3 = 2 x 2 x 3 x 2 = 2 x 3 x 2 x 2 = 3 x 2 x 2 x 2. Em resumo, $24 = 2^3 \times 3$

Teorema 2 (Teorema Fundamental da Aritmética)
Todo número inteiro maior do que 1 se escreve como o produto único de números primos, a menos da ordem desses fatores primos.
Demonstração 3

Vamos imaginar que o Teorema Fundamental da Aritmética não seja verdadeiro. Desse modo, existiriam alguns (ou algum) números inteiros maiores do que 1 que não se escreveriam com o produto de primos, de modo único.
Seja n o *menor* inteiro maior do que 1 para o qual o teorema não fosse verdadeiro. O número *n,* ele próprio, não pode ser primo, pois, nesse caso, ele seria a sua própria decomposição em fatores primos (um só fator). Portanto, n seria composto e poderíamos escrever $n = ab$, com $0 < a < n$ e $0 < b < n$. Nesse caso, a e b podem ser decompostos em produtos de primos, pois ambos são menores do que n, que é, por hipótese, o menor número que não pode ser decomposto como produto de primos. Logo, teríamos:

$a = p_1.p_2.p_3.p_4.....p_n$, onde $p_1, p_2, p_3, p_4, ..., p_n$ são números primos não necessariamente distintos, e
$b = q_1.q_2.q_3.q_4.....q_m$, onde $q_1, q_2, q_3, q_4, ..., q_m$ são números primos não necessariamente distintos.

Portanto, $n = ab = p_1.p_2.p_3.p_4.....p_n.q_1.q_2.q_3.q_4.....q_m$, e teríamos n escrito como um produto de primos. Isso é uma contradição com a escolha de *n.*. A contradição vem do fato de assumirmos que existia algum inteiro maior do que 1 para o qual o teorema não fosse válido. Logo, todo número inteiro maior do que 1 se escreve como produto de números primos.

Resta mostrar que os primos que comparecem na decomposição do número n são únicos, a menos da ordem com que comparecem nessa decomposição.
Vamos supor que a decomposição não seja única. Seja *n* o *menor* inteiro maior do que 1 que não se escreve de forma única como produto de primos. Ou seja, existem números primos $p_1, p_2, p_3, p_4, ..., p_n$ e $q_1, q_2, q_3, q_4, ..., q_m$, tais que $n = p_1.p_2.p_3.p_4.....p_n$ e $n = q_1.q_2.q_3.q_4.....q_m$, com $q_1 \leq q_2 \leq ... \leq q_m$.

Logo, $p_1.p_2.p_3.p_4.....p_n = q_1.q_2.q_3.q_4.....q_m$. Se algum p_i for igual a algum q_j, poderíamos dividir ambos os lados da igualdade por p_i, obtendo duas fatorações iguais e contradizendo a minimalidade de n . Assim, todos os $p_i \neq q_j$, para todo i $\in$ {1, 2, 3, ...n} e todo j $\in$ {1, 2, 3, ..., m}. Podemos supor que $p_1 < q_1$. Chamando $Q = q_2.q_3.q_4.....q_m$, tem-se $p_1Q < q_1Q = n$, pois $p_1 < q_1$. Logo, $0 < n - p_1Q < n$. Como n é suposto ter duas decomposições distintas, o número A seguinte pode ser escrito de duas maneiras, a saber:

$A = q_1q_2....q_m - p_1Q = q_1Q - p_1Q = (q_1 - p_1)Q$ e como

$q_1.q_2.q_3.q_4.....q_m = n = p_1.p_2.p_3.p_4.....p_n$, então, também:

$$\mathbf{A} = p_1 p_2 ... p_n - p_1 Q = p_1 (p_2 p_3 .... p_n - Q).$$

Como $p_1 < q_1 \;\; e \;\; p_1 \neq q_j$, $j = 1,2,3,....,m$, então, Q não tem p_1 como fator primo. Também $q_1 - p_1$ não tem p_1 como primo, do contrário p_1 dividiria q_1, o que é uma contradição, pois os dois são números primos distintos. Desse modo, o número $0 < A < n$ admite na segunda decomposição anterior p_1 como fator primo e na primeira decomposição não tem, contrariando a escolha do número *n*.

Observe que o Teorema 2 é fundamental para a Aritmética justamente porque assegura que todo número inteiro maior do que 1 se escreve, de modo único, como produto de primos, a menos da ordem desses fatores primos.

Exemplo 2
Decomponha em fatores primos o número inteiro 120.
Solução

O número dado se escreve (ou se decompõe) como produto de primos da seguinte maneira: 120 = 2.2.2.3.5 . Na prática, escrevemos: $120 = 2^3.3.5$, onde $2 < 3 < 5$.

Exemplo 3
Decomponha em fatores primos o número inteiro 4.667.544.
Solução

O número dado se escreve (ou se decompõe) como produto de primos da seguinte maneira: 4.667.544 = 2.2.2.3.3.3.3.7.7.7.7. Na prática, escrevemos: $4.667.544 = 2^3.3^4.7^4$, onde $2 < 3 < 7$.

Exercício 2
Escreva 63 com produto de números primos.

De um modo geral, como conseqüência do Teorema Fundamental da Aritmética, temos que, se n é um inteiro maior do que 1, que se decompõe em fatores primos distintos $p_1, p_2, p_3, p_4, ..., p_k$, com p_1 aparecendo a_1 vezes, p_2 aparecendo a_2 vezes,....., p_k aparecendo a_k vezes, então, podemos escrever n, de forma única, como

$$n = p_1^{a_1}.p_2^{a_2}.p_3^{a_3}...p_k^{a_k}, \quad \text{onde} \quad p_1 < p_2 < p_3 < .... < p_k .$$

Exemplo 4
Escreva cada um dos números 360, 540 e 700, de forma única, como produto de primos $p_1^{a_1}.p_2^{a_2}.p_3^{a_3}...p_k^{a_k}$, onde $p_1, p_2, p_3, p_4, ..., p_n$ são números primos com $p_1 < p_2 < p_3 < .... < p_k$.
Solução

$360 = 2.2.2.3.3.5. = 2^3.3^2.5$;
$540 = 2.2.3.3.3..5 = 2^2.3^3.5$;
$700 = 2.2.5.5.7 = 2^2.5^2.7$

Exercício 3
Escreva 80 como produto de números primos $p_1^{a_1}.p_2^{a_2}.p_3^{a_3}...p_k^{a_k}$, onde $p_1, p_2, p_3, p_4, ..., p_k$ são números primos com $p_1 < p_2 < p_3 < .... < p_k$.

Na aula 5 – O Máximo Divisor Comum, o Mínimo Múltiplo Comum e as equações diofantinas lineares – estudaremos o conceito e as propriedades do Máximo Divisor Comum de dois inteiros. Veremos que o Máximo Divisor Comum de dois inteiros *m* e *n,* que notaremos por MDC(*m, n*), é um inteiro *d* maior do que 1, tal que:

(i) *d* divide *m* e *d* divide *n (*Isto é, *d* é um divisor comum)*;*
(ii) se existe um inteiro *c* maior do que 1, tal que *c* divide *m* e *c* divide *n*, então, $c \leq d$ *(*isto é, *d* é o maior divisor comum).

Podemos usar a decomposição de um número inteiro maior do que 1 como produto de números primos para encontrar o Máximo Divisor Comum de dois inteiros positivos. A título de ilustração, consideremos os números 1890 e 360 e suas decomposições em fatores primos

$1990 = 2 . 3^3 .5.7$ $\qquad$ $360 = 2^3 .3^2 .5$

Observamos que os fatores primos comuns na decomposição dos dois números são 2 , 3 e 5. Para encontrar o MDC(1890, 360), basta agora **multiplicar *os fatores* primos comuns elevados aos menores expoentes**, isto é, MDC(1890, 360) = $2.3^2 .5 = 90$. Outro exemplo, para calcular MDC(150, 280), decompomos os dois números em fatores primos:

$150 = 2.3.5^2$ e $280 = 2^3.5.7$,

e consideramos o ***produto dos fatores primos comuns elevados aos menores expoentes***:

MDC(150, 280) = 2.5 = 10.

De um modo geral, se MDC(*m, n*) = *d*, então, na decomposição de *d* em fatores primos comparecem os fatores primos comuns aos números inteiros *m* e *n.* Como *d* é o maior divisor comum a *m* e *n*, então, cada fator primo comum comparece com o menor expoente.

Exemplo 5
Use o Teorema Fundamental da Aritmética para calcular o MDC dos números: 68 e 120.
Solução

Decompondo ambos os números dados, obtemos: $68 = 2^2$ x 17 e $120 = 2^3$ x 3 x 5. Logo, o único primo comum na decomposição dos dois números dados é 2 e o menor expoente é 2. Portanto, MDC(68, 120) = $2^2 = 4$.

Usualmente, para decompor um número inteiro positivo n em fatores primos, usamos o algoritmo para fatores primos, que é a divisão por todos os primos que dividem n. No algoritmo, aparece o número, seus divisores e o respectivo quociente. Os divisores estão na coluna à direita, em ordem decrescente do número e na coluna do número estão os respectivos quocientes. Por exemplo, a decomposição em fatores primos de 12 é feita do modo seguinte:

12	2
6	2
3	3
1	

que significa $12 = 2.2.3 = 2^2.3$.

Veja a decomposição de 360 em fatores primos:

360	2
180	2
90	2
45	3
15	3
5	5
1	

que significa $360 = 2.2.2.3.3.5 = 2^3.3^2.5$.

Exercício 4
Use o Teorema Fundamental da Aritmética para calcular o MDC dos números:
(a) 258 e 828 (b) 60 e 144

Uma pergunta: quantos são os divisores positivos de um número natural n?

Para facilitar o entendimento, vamos particularizar a pergunta: **quantos são os divisores positivos de 12?**

Para responder, precisamos descrever um divisor positivo de 12. Para isso, vamos utilizar o Teorema Fundamental da Aritmética no caso em que $n = 12$. Isto é, $12 = 2^2.3$. Um divisor positivo de 12 é um número d para o qual só comparece na sua decomposição em fatores primos os números primos 2 e 3. Além disso, d só pode ter o 2 como fator primo se 2 estiver elevado a: 0,1 ou 2. Do mesmo modo, o divisor d só pode ter o fator 3 elevado a: 0 ou 1. Desse modo, a quantidade de divisores positivos de 12 é $3.2 = 6$. Ou seja, a quantidade

de divisores positivos depende dos expoentes dos primos que comparecem na decomposição do número em fatores primos. Assim, podemos concluir que são os seguintes os divisores positivos de 12:

$$1 = 2^0.3^0; \quad 2 = 2^1.3^0; \quad 3 = 2^0.3^1; \quad 4 = 2^2.3^0; \quad 6 = 2^1.3^1; \quad 12 = 2^2.3.$$

De uma maneira geral, se n é um número inteiro maior do que 1 e $n = p_1^{a_1}.p_2^{a_2}.p_3^{a_3}...p_k^{a_k}$, onde $p_1, p_2, p_3, p_4, ..., p_k$ são números primos com $p_1 < p_2 < p_3 < .... < p_k$, então, pelo Princípio Multiplicativo (veja na aula 1 – Aprendendo a

contar – da disciplina Análise Combinatória) o número de divisores positivos de n é igual a: $(a_1+1).(a_2+1)(a_3+1)...(a_k+1)$.

Exemplo 6
Quantos são os divisores positivos de 540?
Solução

Pelo que vimos anteriormente, a decomposição de 540 em fatores primos é:

540	**2**
270	**2**
135	**3**
45	**3**
15	**3**
5	**5**
1	

Ou seja, $540 = 2^2.3^3.5$ e todo divisor positivo de 540 é da forma $d = 2^a.3^b.5^c$, onde

$a \in \{0, 1, 2\}$, $b \in \{0, 1, 2, 3\}$ e $c \in \{0, 1\}$. Desse modo, usando o Princípio Multiplicativo, a quantidade de divisores positivos de 540 é igual a $(2 + 1).(3 + 1).(1 + 1) = 24$.

Exercício 5
Quantos divisores positivos possui o número 2^{100}?

Exercícios

1) Com relação ao número 375:
(a) escreva 375 como produtos de números primos;
(b) descreva a expressão geral dos divisores de 375;
(c) quantos e quais são os divisores de 375?

2) Um número inteiro é chamado *livre de quadrado* se ele não é divisível pelo quadrado de algum primo.
(a) Dê 5 exemplos de inteiros positivos compostos, cada um sendo *livre de quadrado*.

(b) Usando o Teorema Fundamental da Aritmética, diga a forma geral na qual pode ser escrito cada inteiro positivo maior do que 1 que seja livre de quadrado.

3) Considere o seguinte número inteiro maior do que 1: $z = n^4 + 4$, onde n é um número natural. Diga, justificando, se z é um número primo.

Sugestão – Pense numa fatoração do binômio $n^4 + 4$ como produto de dois trinômios do segundo grau.

4) São dados dois números naturais, m e n, tais que MDC(m, n) = 15.

(a) Quais são os primos comuns que fazem parte da decomposição de m e n em fatores primos?

(b) Qual é o menor expoente de cada um dos primos comuns que comparecem na decomposição de m e n?

5) Maria escreve num pedaço de papel os cubos de três inteiros positivos. Antônio verifica que cada um deles é múltiplo de 18 e que o Máximo Divisor Comum dos cubos desses números é n. Encontre o menor valor possível para n.

6) Com relação ao número 160, faça o que se pede.

(a) Escreva 160 como produto de números primos.
(b) Descreva a expressão geral dos divisores de 160.
(c) Quantos e quais são os divisores de 160?

7) Use o Crivo de Eratóstenes para encontrar todos os primos menores do que ou iguais a 200.

8) Qual é a soma de todos os inteiros positivos menores do que 100 que têm exatamente 12 divisores?

9) Sabendo que MDC(m, n) = 1 e que m e n possuem, respectivamente, 8 e 12 divisores positivos, quantos divisores possui o número mn?

10) Certo número natural K tem exatamente oito divisores, dentre os quais estão 35 e 77.
Encontre o número K.

11) O número natural $(2^{48} - 1)$ é divisível por dois números entre 60 e 70. Encontre esses números.

Sugestão – Use produtos notáveis para decompor $(2^{48} - 1)$.

12) Responda as questões a seguir.

(a) Usando o Teorema Fundamental da Aritmética, prove que $\sqrt{2}$ não é um número racional.
(b) Usando o Teorema Fundamental da Aritmética, prove que $\sqrt{3}$ não é um número racional.
(c) Adaptando seus argumentos usados nos subitens (a) e (b), é possível provar que o número $\sqrt{p}$, com p número primo, não é um racional?

13) Leia o enunciado a seguir e responda as questões.

Escreve-se no quadro-negro os números inteiros de 1 a 100. Dois jogadores disputam o seguinte jogo, em que jogam alternadamente. Uma jogada consiste em apagar um dos números escritos. O jogo termina quando restam somente dois números no quadro-negro. O primeiro jogador vence se a soma desses dois números é divisível por 3; o segundo jogador ganha caso ocorra o contrário.

a) Quem vence: o primeiro ou o segundo jogador?

b) Qual a estratégia usada para vencer?

Sugestão – O número 101 não é divisível por 3. Veja como 101 pode ajudá-lo a definir uma estratégia vencedora.

Resumo

Nesta aula, estudamos o papel importante dos números primos dentro do conjunto dos números inteiros, culminando com o Teorema Fundamental da Aritmética, o qual diz que cada número natural maior do que 1 pode ser decomposto, de forma única, como produto de fatores primos, a menos da ordem desses fatores.

Problemas Suplementares

Problema 1

O número 27.000.001 possui exatamente quatro fatores primos.
Encontre a soma desses fatores primos.

Sugestão: $27x^6 + 1 = (3x^2)^3 + 1 = (3x^2 + 1).(3x^2 + 3x + 1).(3x^2 - 3x + 1)$.

Problema 2

Existem quantos inteiros positivos com 2 dígitos (na base 10), tendo um número par de divisores?
Resp. 84

Problema 3

Encontre o menor inteiro positivo que é duas vezes um quadrado perfeito e três vezes um cubo perfeito.
Resp. 648

Problema 4

Um inteiro positivo n é chamado "*cintilante"* se seu menor inteiro positivo maior do que 1 é igual à quantidade de divisores positivos de n. O número 9 é cintilante, pois os divisores positivo de 9 são: 1, 3 e 9, sendo 3 o menor divisor positivo maio do que 1.
Quantos são os números cintilantes?

Resp. 3

Problema 5

Encontre todos os números inteiros positivos n para os quais $3^{512} - 1$ seja divisível por 2^n.

Resp. 11

Problema 6

Existem quantos números inteiros positivos a, com $1 \le a \le 200$, tais que a^a é um quadrado?

Resp. 107

Problema 7

Existem quantos pares de inteiros (a,b), com $1 \le a \le b \le 60$, tendo a propriedade de que b é divisível por a e $b + 1$ é divisível por $a + 1$?

Resp. 30

Problema 8
Identifique o inteiro positivo n, menor do que 1000, que possui exatamente 29 divisores positivos, sem contar ele próprio.
Resp. 720

Problema 9
Cada noite, três pessoas de um grupo de n pessoas saem juntas para jantar. Depois de certo período de tempo se observa que cada para de pessoas jantam junto exatamente uma vez. Demonstre que n deixa resto 1 ou 3 na divisão por 6.

Referências

BURTON, David M. **Elementary number theory**. New York: McGraw-Hill, 1998.

COUTINHO, S. C. **Números inteiros e criptografia RSA**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada – IMPA/ Sociedade Brasileira de Matemática – SBM, 1997.

DU SAUTOY, Marcus. **A música dos números primos**: a história de um problema não resolvido. Rio de Janeiro: Jorge Zahar, 2008.

HEFEZ, Abramo. **Elementos de aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2005.

PERELMÁN, Ya I. **Problemas y experimentos recreativos**. Moscú: Editorial MIR, 1975.

Aula 5 – O máximo divisor comum, o mínimo múltiplo comum e as equações diofantinas lineares

Apresentação

Nesta aula, estudaremos o Máximo Divisor Comum entre dois inteiros e veremos como Euclides usou esse conceito para provar resultados da Teoria dos Números.

Não espere encontrar um grau de dificuldade uniforme. Umas coisas são mais difíceis que outras. Nelas, você tem que gastar mais tempo. Não fique impaciente. Leia várias vezes o que julgar mais difícil. Veja cuidadosamente os exemplos, pois eles servem de referência para você consolidar a aprendizagem.

Objetivos

- Calcular o Máximo Divisor Comum e o Mínimo Múltiplo Comum.
- Calcular o Máximo Divisor Comum usando o Algoritmo de Euclides.
- Escrever o Máximo Divisor Comum de dois números inteiros m e n como combinação linear de m e n.
- Resolver Equações Diofantinas Lineares como aplicações do Máximo Divisor Comum.

O máximo divisor comum

O número inteiro 4 divide 12 e 4 também divide 20 e, além disso, como você pode verificar facilmente, 4 é o maior número inteiro positivo com essa propriedade. Dizemos, então, que 4 é o **Máximo Divisor Comum** de 12 e 20, e notamos 4 = MDC(12, 20).

De uma maneira geral, o número inteiro positivo d é o **Máximo Divisor Comum** de dois números inteiros a e b se d é o maior número positivo que divide a e b ao mesmo tempo. Isso pode ser precisado nos itens abaixo:

(i) d divide a e d divide b (i.e. d é um divisor comum);
(ii) se existe um número natural c tal que c divide a e c divide b, então $c \leq d$ (i.e. d é o maior divisor comum).

Notaremos isso por: MDC(a, b) = d.

Veja que, por definição, o MDC é sempre um número positivo.

Observe que os inteiros 5 e 7 não possuem divisores positivos comuns, exceto o 1. Nesse caso, MDC(5, 7) = 1 e dizemos que 5 e 7 são **primos entre si** (ou que 5 e 7 **são relativamente primos**).

De uma maneira geral, dois números naturais *a* e *b* são **primos entre si** (ou **relativamente primos**) se MDC(a, b) = 1.

Podemos usar o Algoritmo da Divisão para calcular o Máximo Divisor Comum de dois números naturais. O método consiste em fazer sucessivas aplicações do Algoritmo da Divisão até obter o resto nulo. Ilustramos o método com o exemplo seguinte.

Exemplo 1
Usando o Algoritmo da Divisão, calcular o MDC(360, 126).
Solução

Usando o Algoritmo da Divisão, dividimos 360 por 126 escrevendo

360 = 2 x 126 + 108 (2 é o quociente e 108 é o resto).

Agora, como o resto da divisão não é nulo, aplicamos novamente o Algoritmo da Divisão para o divisor inicial e o resto da divisão anterior, ou seja,

126 = 1 x 108 + 18 (1 é o quociente e 18 é o resto).

Como o resto da última divisão ainda não é nulo, procedemos como da vez anterior, dividindo o divisor acima pelo resto obtido, isto é:

108 = 6.18 + 0 (6 é o quociente e 0 é o resto).

Como o resto da última divisão é nulo, então o divisor 18 é o Máximo Divisor de 360 e 126, isto é MDC(360, 126) = 18, conforme veremos na Proposição 1.

Ilustramos os cálculos anteriores no diagrama a seguir:

	1	6	← **quocientes**
126	108	**18**	
18	0		← **restos**

Exemplo 2
Usando o Algoritmo da Divisão, calcular o MDC(32, 12) = 4.

Solução

Usando o Algoritmo da Divisão, o cálculo correspondente é

32 = 2 x 12 + 8
12 = 1 x 8 + 4

$$8 = 2 \times 4 + 0,$$

ou seja:

	2	1	2	← **quocientes**
32	12	8	**4**	
8	4	0		← **restos**

Como no Exemplo 1, conclui-se que o MDC(32, 12) = 4.

Exercício 1
(a) Encontre o quociente *q* e o resto r na divisão de 72 por 20.
(b) Ache o MDC(72, 20).
(c) Ache o MDC(20, r).
(d) Compare o MDC(72, 20) e MDC(20, r).

O procedimento descrito nos Exemplos 1 e 2 é correto, pois é uma aplicação repetida do fato seguinte, que é verdadeiro, como veremos a seguir:

Proposição 1
Se a e b são dois números naturais, de acordo com o Algoritmo da Divisão, existem naturais, q e r tais que b = q. a + r, com $0 \leq r < a$. Nesse caso, MDC(a, b) = MDC(a, r).
Demonstração

Se MDC(*a,b*) = *d*, então $d \mid a$ e $d \mid b$. Logo, $a = d.u$ e $b = d.b$, *com u, v* números inteiros. Como existem inteiros *q* e *r* tais que $b = q.a + r$, segue que $r = b - qa = d.v - qdu = (v - qu).d$. Portanto, $d \mid r$. Assim, *d* é um divisor comum de *b* e *r*. Resta mostrar que *d* é o maior divisor comum de *b* e *r*. Suponha que existe um inteiro positivo *c* tal que $c \mid a$ e $c \mid r$. Como $b = q.\ a + r$, segue que $c \mid b$. *Como d* = MDC(*a, b*) e *c* é um divisor comum de a e b, então $d \geq c$. Portanto, *d* = MDC(*b, r)*.

De acordo com a Proposição 1, para encontrar o MDC(*a,b*) fazemos repetidas aplicações do Algoritmo da Divisão até obter um resto zero, caso em que o penúltimo resto é o *MDC(a, b)*. Outra conclusão que poderemos tirar, a partir do uso do Algoritmo da Divisão, é: o Máximo Divisor Comum de *a* e *b* é uma **combinação linear de *a* e *b***, isto é:

MDC(*a, b)* = $ax + by$, com *x, y* inteiros.

Para exemplificar, quando calculamos anteriormente o MDC(360, 126) = 18, aplicamos três vezes o Algoritmo da Divisão. Agora, explicitando o valor de 18 na segunda igualdade, obtemos:

$$18 = 126 + (-1).108.$$

Isolando o valor de 108 na primeira aplicação do Algoritmo da Divisão e substituindo na igualdade acima, obtemos:

MDC(360, 126) = 18 = 3.126 + (-1).360

ou seja, para expressar o Máximo Divisor Comum entre dois números, usamos o Algoritmo da Divisão "ao inverso", isto é, aplicamos o Algoritmo da Divisão até encontrar o resto 0 e vamos desfazendo até encontrar os dois números.

De uma maneira geral, podemos afirmar:

Teorema 1 (Bachet – Bezout)
Dados a e b números inteiros (ambos não nulos), então existem inteiros x e y tais que MDC(a, b) = ax + by.
Demonstração

Para facilitar a prova, considere S a coleção de todas as combinações lineares inteiras positivas de *a* e *b*. Ou seja,

$$S = \{ ax + by \mid x \text{ e } y \text{ são inteiros e } ax + by > 0\}.$$

Vamos mostrar que S é não vazio e, portanto, possui um menor elemento *m*. Provaremos que este menor elemento $m \in S$ é o *MDC(a, b).*
Se $a > 0$, podemos escrever $a = a.1 + 0.b$, o que mostra que *a* está em S. Por outro lado, se $a < 0$, podemos escrever $-a = a.(-1) + b.0$, o que mostra que *-a* está em S. Assim, podemos concluir que S é um conjunto não vazio de inteiros positivos. Pelo Princípio do Menor Inteiro, S possui um menor elemento. Seja *m* este menor elemento de S. Logo, existem *u* e *v* inteiros tais que $m = au + bv$.

O que vamos fazer a seguir é, utilizando o Algoritmo da Divisão, dividir *m* por *a* e *b* e mostrar que em ambos os casos o resto é zero. Ou seja, $m \mid a$ e $m \mid$ b. De fato, como $a = q.m + r$, onde $0 \leq r < m.$, temos que $r = a – q.m = a – q.(au + bv) = a(1 – qu) + b(qv)$. Se $r \neq 0$, temos que *r* está no conjunto S. Mas, $r < m$, e *m* é o menor elemento de S. Contradição. Logo, $r = 0$. E, portanto, $m \mid a$.

Argumentando de maneira análoga, prova-se que $m \mid$ b.
Agora, segue que $m \leq d$ = MDC(*a, b*). Por outro lado, como $m = au + bv$, com *u, v* inteiros e *d* divide *a* e *b,* segue que $d \mid m$. Portanto, $d \leq m$.
Assim, $m = d$ = MDC(*a, b*).

A demonstração do Teorema de Bachet-Bezout não fornece uma pista de como encontrar x e y inteiros para que se tenha $d = ax + by$. Apesar dessa deficiência, esse resultado é muito útil, como veremos no restante desta aula.

Segue do Teorema de Bachet-Bezout, os seguintes corolários:

Corolário 1
Se *d* = MDC(*a, b*), então qualquer divisor *c* de *a* e *b* divide *d.*
Demonstração

Se d = MDC(a, b), então existem x e y inteiros para os quais $d = ax + by$. Como c divide a e c divide b, então a = c.t e $b = c.v$, com t, v inteiros, tem-se $d = ax + by = ctx + c.vy = c(tx + vy)$. Em resumo, d = ck, onde k = tx + vy, o que implica que c divide d.

Corolário 2
Os inteiros a e b não nulos são **relativamente primos** se, e somente se, x e y pertencem aos inteiros tais que ax + by = 1.
Demonstração

Se a e b são dois números inteiros não nulos e relativamente primos, então $MDC(a, b) = 1$. Pelo resultado acima, existem x e y pertencentes aos inteiros tais que $ax + by = MDC(a, b) = 1$.
Reciprocamente, se existem x e y inteiros, com $ax + by = 1$, então todo divisor d de a e b divide $ax + by = 1$, isto é, d divide 1. Logo, $d = 1$. Portanto, a *e* b são relativamente primos.

Exemplo 3
Encontrar inteiros x e y tais que $MDC(3, 20) = 3x + 20y$.
Solução

Usando o Algoritmo da Divisão, 20 = 6.3 + 2; 3 = 1.2 + 1 e 2 = 2.1 + 0. Logo, $MDC(3, 20) = 1$. Assim, existem x e y pertencentes aos inteiros tais que $3x + 20y = 1$. Veja que $x = 7$ e $y = -1$ verifica a igualdade.

Exercício 2
Em cada item a seguir, encontre quatro pares de inteiros (m, n) tais que :
(a) MDC(2, 3) = $2m + 3n$
(b) MDC(24, 51) = $24m + 51n$
(c) MDC(72,164) = $72m + 164n$

Sendo o Máximo Divisor Comum definido para dois números inteiros, entendemos MDC (a, b, c), com a, b e c números inteiros, como sendo:

MDC ($a, MDC(b,c)$) = MDC($MDC(a, b), c) = ($MDC($a, c), b)$.

Ilustrando,
MDC(39, 42, 54) = MDC(MDC(39, 42), 54) = MDC(3, 54) = 3 ou
MDC (39, 42, 54) = MDC(39, MDC(42, 54)) = MDC (39, 6) = 3.

Agora, vamos provar o seguinte resultado, citado na aula 2 (Divisibilidade):

Teorema 2 (Euclides)
Se um número primo p divide o produto de dois números naturais a.b, então p divide a ou p divide b.
Demonstração

Vamos supor que p não divide a. Nesse caso, como p é um número primo, p e a são relativamente primos. Logo, MDC$(a, p) = 1$. Portanto, existem números inteiros x e y tais que MDC$(a, p) = 1 = ax + py$. Multiplicando ambos os lados da (última) igualdade por b, obtemos

$abx + bp\ y = b$. Como, por hipótese, $p| ab$, temos que: $ab = pk$, onde k é um número inteiro. Assim, $b = abx + bp\ y = pkx + bpy = p(kx + by)$. Portanto, p divide b. De modo análogo, supondo que p não divide b, conclui-se que p divide a.

Exemplo 4
O número 7 divide o produto 84 x 12 = 1.008. Como 7 não divide 12, segue que 7, obrigatoriamente, divide 84. De fato, 84 = 12 x 7.

Observe que, se o número p não for primo, o Teorema 1 não é verdadeiro. De fato, 12 não é primo e 12 divide o produto 8 x 15. Mas, 12 não divide 8 nem divide 15.

Ou seja, no Teorema 1, a hipótese de p ser um número primo é **indispensável**.

O mínimo múltiplo comum

Observe que 6 divide 60 e 15 divide 60. Nesse caso, 60 é dito um múltiplo comum de 6 e 15. Do mesmo modo, 8 divide 120 e 20 divide 120. Assim, dizemos que 120 é um múltiplo comum de 8 e 20.

De uma maneira geral, se a é um número inteiro que divide o inteiro m, dizemos *que m é* um **múltiplo *de a.***

Se a e b são números inteiros não nulos, então podemos concluir que tanto ab como $-ab$ são múltiplos comuns de a e b e um deles tem de ser positivo (pelo Axioma da Tricotomia, visto na aula 2). Portanto, pelo Princípio do Menor Inteiro, existe um menor múltiplo comum de a e b. Seja m este número positivo que é o menor múltiplo comum de a e b. Chamamos m de **Mínimo Múltiplo Comum** de a e b, e notamos por m = MMC(a, b).

Resumindo, m = MMC(a, b) se, e somente se,

(i) m é um inteiro positivo;
(ii) a divide m e b divide m (m é um múltiplo comum de a e b);
(iii) Se n é um múltiplo de a e b, então $n \geq m$ (m é o menor múltiplo comum).

Exemplo 5
O MMC (12, 30) é 60, pois
(i) 60 é um inteiro positivo;
(ii) 12 divide 60, pois 60 = 12 . 5, e 30 divide 60, pois 60 = 30 . 2;
(iii) 60 é o menor múltiplo comum de 12 e 30.

Exercício 3
Ache:
(a) MMC(12, 42) (b) MMC(18, 32)

Existe uma relação entre o MDC e o MMC dada por:

Proposição 2
Se a e b são dois números inteiros positivos, então: MDC (a, b) x MMC (a, b) = ab.
Demonstração

De fato, seja d = MDC (a, b). Como d é um divisor de a e b, podemos escrever: $a = dm$ e $b = dn$, com $m, n \in \mathbf{Z}$. Se s = ab/d, então s = $dmb/d = bm$ e s = $adn/d = na$. Portanto, s é um inteiro positivo que é múltiplo de a e b. Precisamos mostrar que s é o Mínimo Múltiplo Comum de a e b. Para isso, suponha que outro número inteiro positivo r seja um múltiplo comum de a e b. Assim, podemos escrever $r = au$ e $r = bv$, com $u, v \in \mathbf{Z}$. Por outro lado, sabemos, pelo Teorema 1, que existem inteiros x e y tais que $d = ax + by$. Logo, podemos escrever:

$\frac{r}{s} = \frac{rd}{sd} = \frac{r(ax+by)}{ab} = \left(\frac{r}{b}\right)x + \left(\frac{r}{a}\right)y = (vx+uy) \in Z$. Portanto, s divide r. Em particular, $s \leq r$. Logo, podemos concluir que s = MMC (a, b). *Como* $s = \frac{ab}{d}$ *então* $ds = ab$, *isto é,* $MDC(a, b).\ MMC(a, b) = ab$

Corolário 3
Se MDC (a, b) = 1, temos, $MMC\ (a, b) = ab$.
Demonstração

Da Proposição 2, temos **MDC (a, b) x MMC (a, b) = ab.** Como, por hipótese, MDC (a, b) = 1, segue que MMC (a, b) = ab.

Exemplo 6
Achar MMC(72, 20).
Solução

Basta observar que MDC(72, 20) = 4 e aplicar a Proposição 2:
MDC(72, 20) x MMC(72, 20) = 72 x 20.
Assim, 4 x MMC(72, 20) = 72 x 20. Portanto, MMC(72, 20) = $\frac{72\,x\,20}{4} = 360$.

Exercício 4
Encontre MMC(120, 36).

Equações diofantinas lineares

É usual chamar **equações diofantinas** as equações com coeficientes inteiros e com uma ou mais incógnitas a serem procuradas no conjunto dos números inteiros. As mais simples são as **equações diofantinas lineares**:

$ax + by = c$, com a, b, c constantes e $a, b, c \in \mathbf{Z}$.

A solução de uma equação diofantina desse tipo são dois inteiros x_0, y_0, tais que $ax_0 + by_0 = c$.

As equações seguintes são diofantinas: $3x + 8y = 9$; $4x + 30y = 42$; $x + y = 1$.

O nome dessas equações é em homenagem a Diofanto, que iniciou estudos no sentido de resolvê-las e que tomamos conhecimento através de **Os Elementos,** de Euclides. Diofanto viveu em Alexandria por volta de 250 depois de Cristo.

Diofanto de Alexandria é considerado como o maior algebrista grego. Na história da Aritmética, esse autor desempenha um papel semelhante ao que Euclides (360-295 aC) tem na Geometria e Ptolomeu (85-165) na Astronomia. Sabe-se relativamente pouco sobre a sua vida. Desconhece-se a data precisa em que Diofanto nasceu. No entanto, através da leitura dos seus escritos, nos quais cita Hipsicles (240-170 a.C.) e também por uma passagem de Théon de Alexandria (335-395), que cita Diofanto como um clássico, é possível marcar limites temporais que permitem situar a vida desse autor entre o Século II a.C. e o princípio do Século IV da nossa Era. De acordo com P. Tannery, deve-se considerar Diofanto como contemporâneo de Papus (290-350) e pertencendo à segunda metade do Século III. Por outro lado, atendendo ao que na parte da aritmética da mutilada obra de Papus não é mencionado o nome de Diofanto, sendo, no entanto, citados, não só diversos outros geômetras da época, mas também quase todos os matemáticos do seu tempo como Héron (10-75), Nicómaco (60-120), Théon e Ptolomeu, Diofanto possa ser um pouco posterior a Papus.

Entre os vários livros que escreveu, o mais importante é **"Aritmética"**. Neste, ele introduz uma notação simbólica com símbolos diferentes para o quadrado de uma incógnita, para o cubo e assim sucessivamente.

Em sua tumba estava escrito o seguinte enigma: "Aqui jaz o matemático que passou um sexto da sua vida como menino. Um doze avos da sua vida passou como rapaz. Depois viveu um sétimo da sua vida antes de se casar. Cinco anos após, nasceu seu filho, com quem conviveu metade da sua vida. Depois da morte de seu filho, sofreu mais 4 anos antes de morrer". De acordo com esse enigma, Diofanto teria 84 anos.
(Fonte: http://pt.wikipedia.org/wiki/Diofanto_de_alexandria)

Exemplo 7
$2x + 8y = 10$ é uma equação diofantina e $x = 1$ e $y = 1$ é uma solução, pois $2.1 + 8.1 = 10$. Observe que $x = 5$ e $y = 0$ é outra solução. Assim, de uma maneira geral, as soluções de uma equação diofantina não são únicas

Atenção!
Quando estudamos as equações diofantinas é natural surgir os seguintes questionamentos:

Pergunta 1: toda equação diofantina admite solução?

Resposta: nem toda equação diofantina admite solução. Por exemplo, $4x + 6y = 13$ não admite solução, uma vez que poderíamos escrever, $13 = 4x + 6y = 2(2x + 3y)$. Isso nos diz que 13 é par, o que é uma contradição.

Pergunta 2: que condições devem satisfazer os números inteiros a, b e c para que a equação diofantina $ax + by = c$, admita solução?

Resposta: a equação diofantina ax + by = c, com a, b, c constantes e a, b, c $\in$ **Z** admite solução se, e somente se, o MDC (a, b) divide c. De acordo com esse critério, a equação 4x + 6y = 13 não admite solução porque MDC (4, 6) = 2 e 2 não divide 13.

Pergunta 3: como justificar o critério de solubilidade das equações diofantinas?

Resposta: vamos supor que a equação diofantina $ax + by = c$, com a, b, c constantes e $a, b, c \in \mathbf{Z}$ admita solução. Isso quer dizer que existem inteiros x_0, y_0 tais que $ax_0 + by_0 = c$. Seja d = MDC (a, b). Assim, pelo Teorema 1, existem $r, s \in \mathbf{Z}$ tais que $a = dr$ e $b = ds$. Desse modo, podemos escrever:

$$c = ax_0 + by_0 = drx_0 + ds.y_0 = d(rx_0 + s.y_0).$$

Portanto, d = MDC (a, b) divide c.

Por outro lado, se d = MDC (a, b) divide c, então existe $t \in \mathbf{Z}$ tal que $c = dt$. Já sabemos que existem dois inteiros x_0, y_0 tais que d = MDC (a, b) = $ax_0 + by_0$. Multiplicando ambos os membros desta última igualdade por t, obtemos: $c = dt = (ax_0 + by_0).t = a(tx_0) + b(ty_0)$. Portanto, a equação diofantina admite uma solução $x = (tx_0)$ e $y = (ty_0)$, o que conclui a justificativa de que *a equação diofantina* $ax + by = c$, *com* a, b, c *constantes e* $a, b, c \in \mathbf{Z}$ admita solução se, e somente se, *o MDC (a, b) divide c.*

Exemplo 8
Considere a seguinte equação diofantina 5x + 12 y = 18. Essa equação diofantina admite solução, pois MDC (5, 12) = 1 e 1 divide 18, enquanto a equação diofantina 18x + 12 y = 25 não admite solução, pois MDC (18, 12) = 6, pois 6 não divide 25.

Pergunta: supondo que a equação diofantina ax + by = c, com a, b, c constantes e a, b, c $\in$ **Z** **admite solução**, quais são todas as suas soluções?

A resposta é dada pela Proposição 3.

Proposição 3
Se x_0, y_0 é uma solução particular da equação diofantina ax + by = c, então todas as soluções desta equação são dadas por:

$$x = x_0 + \left(\frac{b}{d}\right)t \quad \text{e} \quad y = y_0 - \left(\frac{a}{d}\right)t, \text{ com } t \text{ um número inteiro.}$$

Demonstração

Sejam x' e y' outra solução qualquer da equação. Assim, temos:

$$ax' + by' = c \quad \text{e} \quad ax_0 + by_0 = c.$$

Portanto, $ax' + by' = ax_0 + by_0$, que é o mesmo que:

$$a(x' - x_0) = b(y_0 - y'). (*)$$

Seja d = MDC (a, b). Sabe-se que existem inteiros, r e s, relativamente primos, tais que $a = dr$ e $b = ds$. Logo, a igualdade *(*)* pode ser reescrita como:

$a(x' - x_0) = b(y_0 - y') = dr(x' - x_0) = ds(y_0 - y')$ ou ainda: $r(x' - x_0) = s(y_0 - y')$.

Como s divide $r(x' - x_0)$ e s é relativamente primo com r, temos que s divide $(x' - x_0)$. Logo,

$$x' - x_0 = st \text{ ou ainda } x' = x_0 + st, = x_0 + \left(\frac{b}{d}\right)t \text{ , com } t \text{ um número inteiro.}$$

Por outro lado, como $r(x' - x_0) = s(y_0 - y_1)$ e $x' - x_0 = st$, então $rst = s(y_0 - y')$. Logo,

$$y_0 - y' = rt, \text{ ou ainda } y' = y_0 - rt = y_0 - \left(\frac{a}{d}\right)t, \text{ com } t \text{ um número inteiro.}$$

Para concluir, basta verificar que, $x' = x_0 + \left(\frac{b}{d}\right)t$ e $y' = y_0 - \left(\frac{a}{d}\right)t$, com t um número inteiro, satisfaz a equação diofantina dada, de fato:

$$ax' + by' = a[x_0 + \left(\frac{b}{d}\right)t\,] + b[y_0 - \left(\frac{a}{d}\right)t\,] = (ax_0 + by_0) + \left(\frac{ab}{d} - \frac{ab}{d}\right)t = (ax_0 + by_0) + 0 = c.$$

Exemplo 9
Por exemplo, $2x + 8y = 10$ é uma equação diofantina e $x = 1$ e $y = 1$ é uma solução particular. Como MDC (2, 8) = 2 = d, $a = 2$ e $b = 8$, todas as soluções são dadas por:

$$x = 1 + \left(\frac{8}{2}\right)t = 1 + 4t \quad \text{e} \quad y = 1 - \left(\frac{2}{2}\right)t = 1 - t, \text{ com } t \text{ um número inteiro.}$$

Exercício 5
Encontre todas as soluções da equação diofantina $7x - 12y = 9$.

Uma pergunta: dada a equação diofantina $172x + 20y = 1000$, como encontrar uma solução particular?

A resposta é: aplicando o Algoritmo da Divisão para encontrar o MDC (172, 20) e trabalhando no sentido inverso para encontrar a solução particular. Ou seja:

172 = 8 x 20 + 12;
20 = 1 x 12 + 8;
12 = 1 x 8 + 4;
8 = 2 x 4 + 0.

Agora, como MDC (172, 20) = 4 e 4 divide 1.000, podemos concluir que a equação diofantina dada tem solução e percorrendo os cálculos no sentido inverso vamos encontrar uma solução particular:

$$4 = 12 – 8 = 12 – (20 – 12) = 2 \text{ x. } 12 – 20 = 2 \text{ x } (172 – 8 \text{ x } 20) = 2 \text{ x } 172 + (-17) \text{ x } 20.$$

Finalmente, multiplicando 250 a cada membro da última igualdade, obtemos:

$$4 \text{ x } 250 = 1000 = 500 \text{ x } 172 + (-4250) \text{ x } 20.$$

Ou seja, $x = 500$ e $y = -4250$ é uma solução particular da equação diofantina dada.

Observação

$x = x_0 + \left(\frac{b}{d}\right)t$ e $y = y_0 - \left(\frac{a}{d}\right)t$, com t um número inteiro, são todas as soluções da equação diofantina $ax + by = c$, com $d = MDC\ (a, b)$ dividindo c. Se $d = 1$, então a solução geral da equação dada é dada por:

$x = x_0 + bt$ e $y = y_0 – at$, para t um número inteiro.

Exemplo 10
Encontrar a solução geral da equação diofantina $3x + 8y = 5$.
Solução

A equação dada tem solução particular $x = -1$ e $y = 1$ e como o MDC(3, 8) = 1, a solução geral é dada por $x = -1 + 8t$ e $y = 1 – 3t$, com t um número inteiro.

Exemplo 11
Um fazendeiro deseja comprar filhotes de pato e de galinha, gastando um total de R$ 1.770,00. Um filhote de pato custa R$ 31,00 e um de galinha custa R$ 21,00.

Quantos de cada um dos dois tipos o fazendeiro poderá comprar?
Solução

Chamemos de x o número de patos comprados e y o número de galinhas. Assim, podemos modelar o problema da seguinte maneira

$$31x + 21y = 1770.$$

Observe que MDC (31, 21) = 1 e que 1 divide 1.770. Logo, a equação tem solução. Vamos encontrar uma solução particular. Para isso, usamos o Algoritmo da Divisão:

$31 = 1.21 + 10;$
$21 = 2.10 + 1;$
$1 = 21 + (-2) .10 = 21 + (-2).[31 + (-1). 21] = 3.21 + (-2).31.$

Multiplicando ambos os lados por 1.770, obtemos:

$1770 = (-3540).31 + (5310).21.$

Portanto, uma solução particular é $x = -3540$ e $y = 5310$. A solução geral da equação é dada por:

$x = -3540 + 21t$ e $y = 5310 - 31t.$

Observe que estamos interessados somente nas soluções positivas ou nulas, pois representam quantidades de animais. Assim, temos que impor as condições seguintes:

$-3540 + 21t \geq 0$ e $5310 - 31t \geq 0.$

Portanto, $21t \geq 3540$ e $31t \leq 5310$, que é o mesmo que: $t \geq 168{,}57$ e $t \leq 171{,}29$. Assim, como t é um número inteiro, temos que $169 \leq t \leq 171$.
Desse modo, as soluções são:

$x = -3540 + 21.169 = 9$ e $y = 5310 - 31.169 = 71$; ou
$x = -3540 + 21.170 = 30$ e $y = 5310 - 31.170 = 40$; ou
$x = -3540 + 21.171 = 51$ e $y = 5310 - 31.171 = 9.$

Essas soluções dizem que o fazendeiro tem três alternativas de comprar:
9 patos e 71 galinhas ou 30 patos e 40 galinhas, ou 51 patos e 9 galinhas.

Exercício 6
Se um estudante tem em seu cofre muitas moedas de 10 e de 25 centavos, de quantas maneiras distintas pode pagar seu lanche que custou R$ 2,65?

EXERCÍCIOS

1) Ache o MDC(1000, 14400) e o MMC (12, 42).

2) (a) Encontre o quociente q e o resto r na divisão de 72 por 20.
(b) Ache MDC(72, 20).
(c) Ache MDC(20,r).
(d) Compare MDC(72, 20) e MDC(20,r).

3) (a) Calcule o MDC(990, 720).
(b) Calcule o MDC(990 – 720, 720).
(c) Compare o resultado do subitem (a) com o do subitem (b).

4) (a) Encontre o valor do inteiro positivo d tal que d = MDC(12, 28).
(b) Expresse d como uma combinação linear de 12 e 28. Isto é, encontre números inteiros u e v tais que $d = 12u + 28v$.
(c) Verifique que o conjunto $S = \{12x + 28y \mid x, y \in \mathbf{Z}\}$ é a coleção dos múltiplos inteiros de d..

5) Usando o fato: se a, b $\in$ **N**, com M.D.C.(a, b) = 1, existem x, y $\in$ **Z** tais que ax + by = 1, verifique que a raiz quadrada de dois não é um número racional.
(Nota: um número racional é da forma a/b, onde a e b são números inteiros, com b diferente de zero).

6) Encontre, se possível, as soluções de cada uma das equações diofantinas:
(a) 28x + 35y = 91 (b) 24x + 15y = 9.

Resumo
Nesta aula, vimos que o MDC entre dois números é o maior divisor comum a esses números, enquanto o MMC entre eles é o menor múltiplo comum de ambos. Vimos também como encontrar soluções de Equações Diofantinas, úteis em modelagem de problemas do cotidiano.

Problemas Suplementares

Problema 1
Uma sequência de inteiros positivos é dada por: $a_1 = 1$ e $a_n = MDC(a_{n-1}, n) + 1$, para $n > 1$.
Calcule a_{2002}.
Resp. 3

Problema 2
Arranjam-se 10 números inteiros positivos em torno de um círculo. Cada número é 1 mais do que o MDC dos dois vizinhos.
Qual é a soma dos dez números?
Resp. 28

Problema 3
Os números naturais m e n são relativamente primos.
Prove que MDC($m + n$, $m^2 + n^2$) ou é 1 ou é 2.
Sugestão: Se d divide $m + n$, então d divide $(m + n)^2 – (m^2 + n^2) = 2mn$. Portanto, d divide $2m(m + n) – 2mn = 2m^2$ e divide $2n(m + n) – 2mn = 2n^2$

Referências

BURTON, David M. **Elementary number theory**. New York: McGraw-Hill, 1998.

COUTINHO, S. C. **Números inteiros e criptografia RSA**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada – IMPA/ Sociedade Brasileira de Matemática – SBM, 1997.

CRAWFORD, Mathew. **Introduction number theory**: the art of problem solving. Alphine: AoPS Incorporated, 2006.

HEFEZ, Abramo. **Elementos de aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2005

Aula 6 – Representação dos números naturais e critérios de divisibilidade

Apresentação

Nesta aula, estudaremos a representação dos números naturais numa base qualquer e destacaremos os casos especiais nas bases 10 e 2. Em seguida, estudaremos os critérios de divisibilidade, que nos permitem decidir se um determinado inteiro é ou não divisível por outro, sem precisar efetuar a divisão. Esses critérios de divisibilidades foram estudados por vários matemáticos como al-Khwarizmi, cujo nome completo era Abu Abdullah Mohammed ben Musa al-Khwarizmi (nasceu por volta do ano 780 depois de Cristo e morreu entre 830 e 850 depois de Cristo), e Leonardo de Pisa (cerca de 1180 – 1250), mais conhecido como Fibonacci, que significa filho de Bonacci, matemático e comerciante da idade média, que escreveu, em 1202, um livro denominado *Liber Abacci* que chegou a nós, graças à sua segunda edição de 1228.

Tente entender tudo que está sendo explicado na aula. Estude com caneta e papel ao lado. Leia com atenção. Se for preciso, leia várias vezes uma linha ou um parágrafo. Seja paciente e procure ter certeza que você entendeu o que (e por que) está fazendo.

Objetivos

- Expandir um número natural numa base qualquer *b*.
- Dada a representação de um número natural na base b, identificar esse número na base 10.
- Decidir, sem efetuar a divisão, quando um inteiro é divisível por: 2, 3, 4, 5, 6, 7, 8, 9, 10, 11...

Sistema de numeração decimal

Para representar os números naturais, os babilônios usavam o sistema sexagesimal, desenvolvido na China e na India, há cerca de 1700 anos antes de Cristo. A partir da publicação do livro de Fibonacci, *Liber Abacci,* o sistema decimal posicional, hoje universalmente adotado, passou a ser difundido na Europa.

No sistema decimal posicional, todo número natural é representado por uma seqüência dos dígitos:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9,

o símbolo 0 (zero) representa a ausência de qualquer outro dígito. O sistema é chamado decimal pelo fato de ter dez símbolos ao todo: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

Num número natural escrito na base decimal ou base 10, cada dígito tem, além de seu valor próprio, um peso que lhe é atribuído em função da posição que ele ocupa nesse número. Esse peso é sempre uma potência de 10, que varia de acordo com as regras abaixo:

a) o algarismo da extrema direita tem peso 1;
b) da direita para esquerda, o algarismo seguinte tem peso 10;
c) o terceiro algarismo, da direita para a esquerda, tem peso 100;

d) o quarto algarismo, da direita para a esquerda, tem peso 1000, e assim por diante.

Seguindo as regras acima, como se representa na base 10 cada número natural?

Vamos começar pela representação dos números de 1 até 9. Cada um dos dígitos de 1 até 9 é representado por ele mesmo. O número dez é representado por 10; o número cem é representado por 100; o número mil é representado por 1000 etc. O número 1789 tem a seguinte representação decimal:

$$1 \times 1000 + 7 \times 100 + 8 \times 10 + 9 = 1 \times 10^3 + 7 \times 10^2 + 2 \times 10 + 9.$$

No número mil setecentos e vinte e nove, 1729, o dígito 9, pela posição que ocupa, é chamado o **dígito das unidades**, enquanto o dígito 2 é chamado o dígito das dezenas (pois seu peso é 10), o 7 é o dígito das centenas (pois seu peso é $10^2 = 100$) e o 1 é o dígitos dos milhares (seu peso é $10^3 = 1000$).

O número dois mil e sete, 2007, tem a seguinte representação decimal:

$$2 \times 10^3 + 0 \times 10^2 + 0 \times 10 + 7.$$

O dígito 7 é o dígito das unidades, o primeiro 0, contado da direita para a esquerda, é o dígito das dezenas e o segundo zero é das centenas. O dígito 2 é o dígito dos milhares.

O número 173.648 tem a seguinte representação decimal:

$$1 \times 10^5 + 7 \times 10^4 + 3 \times 10^3 + 6 \times 10^2 + 4 \times 10 + 8.$$

Uma questão: dado um número natural, como obter a sua expansão decimal?

Para exemplificar, suponha que o número dado é 173.648. Inicialmente, o que fazemos é usar o Algoritmo da Divisão, dividindo o número por 10. Em seguida, dividimos o quociente por 10 e assim por diante:

$$\begin{aligned}
173.648 &= 17364 \times 10 + 8 = (1736 \times 10 + 4) \times 10 + 8 = 1736 \times 10^2 + 4 \times 10 + 8 = \\
&= (173 \times 10 + 6) \times 10^2 + 4 \times 10 + 8 = 173 \times 10^3 + 6 \times 10^2 + 4 \times 10 + 8 = \\
&= (17 \times 10 + 3) \times 10^3 + 6 \times 10^2 + 4 \times 10 + 8 = \\
&= 17 \times 10^4 + 3 \times 10^3 + 6 \times 10^2 + 4 \times 10 + 8 = \\
&= (1 \times 10 + 7) \times 10^4 + 3 \times 10^3 + 6 \times 10^2 + 4 \times 10 + 8 = \\
&= 1 \times 10^5 + 7 \times 10^4 + 3 \times 10^3 + 6 \times 10^2 + 4 \times 10 + 8.
\end{aligned}$$

A expansão do número 173.648, acima, é chamada expansão relativa à base decimal, ou seja, relativa à base 10.

É fácil ver que, dados os números naturais m e a, com $a > 1$, existe uma expansão do número m na base a. Isto é, existem inteiros não negativos c_n, c_{n-1},....., c_2, c_1, c_0 $_{(a)}$, todos menores do que a, univocamente determinados, tais que:

$$m = c_n a^n + c_{n-1} a^{n-1} + ...+ c_3 a^3 + c_2 a^2 + c_1 a + c_0 \qquad (*)$$

Basta proceder como fizemos no exemplo acima, quando encontramos a expansão do número 173.648 na base 10, só que agora troca-se o 10 por a. A expansão (*) acima é

chamada a expansão do número m relativo à base a e $c_0c_1c_2...c_{n\,(a)}$ é a representação de m na base a.

Exemplo 1
Seja K um número natural, cuja representação na base 10 é:

$$K = c_n10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2 10^2 + c_1 10 + c_0,$$

com $c_n, c_{n-1}, ..., c_3, c_2, c_1, c_0$ inteiros não negativos, todos menores do que 10.
Mostre que K pode ser escrito como $K = c_0 + 10M$, onde M é um número natural.
Solução

Basta olhar para a representação decimal de K como sendo a soma de duas parcelas:

$$K = c_0 + (c_1 10 + c_2 10^2 + c_3 10^3 + ... + c_n 10^n), \text{ ou ainda:}$$
$$K = c_0 + 10(c_1 + c_2 10 + c_3 10^2 + ... + c_n 10^{n-1}).$$

Chamando $M = c_1 + c_2 10 + c_3 10^2 + ... + c_n 10^{n-1}$, podemos escrever K como sendo

$$K = c_0 + 10M.$$

Exercício 1
Seja K um número natural. Mostre que na representação de K^2 na base 10 o dígito das unidades só pode ser 0, 1, 4, 5, 6 ou 9.

O sistema de base dois

O **Sistema de Base Dois** ou **Sistema Binário** é um sistema numérico que expande valores numéricos usando somente dois símbolos: os dígitos 0 e 1. Isso decorre do fato de que os possíveis restos na divisão por 2 são: 0 e 1. O Sistema Binário é usado por todos os computadores modernos, pois devido à tecnologia empregada o zero representa a ausência de corrente e o 1 a presença de corrente.

Pergunta: Usando somente os dois dígitos, 0 e 1, como fazer para representar todos os números naturais?

Resposta: Do mesmo modo que usamos na expansão de um número natural na base 10, a representação de um número natural na base 2, cada dígito, 0 ou 1, tem um peso que lhe é atribuído em função da posição que ele ocupa nesse número. Esse peso é sempre uma potência de 2, que varia do seguinte modo:

a) o algarismo da extrema direita tem peso 1;
b) da direita para esquerda, o algarismo seguinte tem peso 2;
c) o terceiro algarismo, da direita para a esquerda, tem peso $2^2 = 4$;
d) o quarto algarismo, da direita para a esquerda, tem peso $2^3 = 8$, e assim por diante.

Para escrever os números naturais de um só dígito na base 2, fazemos

$0 = 0$

$1 = 1$

Esses dois números são únicos números naturais representados usando um só dos dígitos 0 e 1. Para escrever os dígitos 2 e 3 na base 2, usamos dois dos dígitos 0 e 1:

Como $2 = 1.2 + 0$ e $3 = 1.2 + 1$, escrevemos $2 = 10_{(2)}$ e $3 = 11_{(2)}$.

Para escrever na base 2 os números de 4 até 7, usamos três dos dígitos 0 e 1:

$4_{(2)} = 100_{(2)}$, pois $4 = 1.2^2 + 0.2 + 0$;
$5_{(2)} = 101_{(2)}$, pois $5 = 1.2^2 + 0.2 + 1$;
$6_{(2)} = 110_{(2)}$, pois $6 = 1.2^2 + 1.2 + 0$;
$7_{(2)} = 111_{(2)}$, pois $7 = 1.2^2 + 1.2 + 1$.

Ainda para exemplificar, para escrever na base 2 os números de 8 a 15, usamos quatro dos dígitos 0 e 1:

$8_{(2)} = 1000_{(2)}$, pois $8 = 1.2^3 + 0.2^2 + 0.2 + 0$;
$9_{(2)} = 1001_{(2)}$, pois $9 = 1.2^3 + 0.2^2 + 0.2 + 1$;
$10_{(2)} = 1010_{(2)}$, pois $10 = 1.2^3 + 0.2^2 + 1.2 + 0$;
$11_{(2)} = 1011_{(2)}$, pois $11 = 1.2^3 + 0.2^2 + 1.2 + 1$;
$12_{(2)} = 1100_{(2)}$, pois $12 = 1.2^3 + 1.2^2 + 0.2 + 0$;
$13_{(2)} = 1101_{(2)}$, pois $13 = 1.2^3 + 1.2^2 + 0.2 + 1$;
$14_{(2)} = 1110_{(2)}$, pois $14 = 1.2^3 + 1.2^2 + 1.2 + 0$;
$15_{(2)} = 1111_{(2)}$, pois $15 = 1.2^3 + 1.2^2 + 1.2 + 1$.

Costuma-se escrever $15 = 1.2^3 + 1.2^2 + 1.2 + 1 = 1111_{(2)}$. Ou seja, $1111_{(2)}$ é a representação de 15 na base 2. Do mesmo modo, $1001_{(2)}$ é a representação de 9 na base 2.

Exemplo 2
Como representamos na base 2 o número 54?
Solução

A representação de 54 na base 2 é feita de modo análogo à sua representação na base 10, porém mudando 10 por 2. Assim, dividimos 54 por dois e, em seguida, dividimos o quociente por 2 e assim por diante, até obter o dividendo como sendo 1:

$54 = 27.2 + 0 = (13.2 + 1).2 + 0 = 13.2^2 + 1.2 + 0 =$
$= (6.2 + 1).2^2 + 1.2 + 0 = 6.2^3 + 1.2^2 + 1.2 + 0 =$
$= (3.2 + 0).2^3 + 1.2^2 + 1.2 + 0 = 3.2^4 + 0.2^3 + 1.2^2 + 1.2 + 0 =$
$= (1.2 + 1).2^4 + 0.2^3 + 1.2^2 + 1.2 + 0 =$
$= 1.2^5 + 1.2^4 + 0.2^3 + 1.2^2 + 1.2 + 0$

Portanto, a representação de 54 na base dois é $110110_{(2)}$.

Exercício 2
Verifique que a representação na base 2 de todo número natural par termina em zero e a representação na base 2 de todo número natural ímpar termina em 1.

Uma pergunta: Como identificar na base 10 o número representado na base 2 por 10101001101?

Resposta: basta atribuir os pesos para cada dígito que comparece na representação do número na base 2 e efetuar a soma:

$1.2^{10} + 0.2^9 + 1.2^8 + 0.2^7 + 1.2^6 + 0.2^5 + 0.2^4 + 1.2^3 + 1.2^2 + 0.2 + 1 = 1357.$

Portanto, $1357 = 10101001101_{(2)}$.

Exercício 3
Se a representação na base 2 do número natural K é $11101011_{(2)}$, qual é a representação na base 2 do número (K +5)?

Exemplo 3
Mostre que se b é um número natural maior do que 2, então, o número $121_{(b)}$ é um quadrado perfeito.
Solução

De fato, $121_{(b)} = 1.b^2 + 2.b + 1 = (b + 1)^2$.

Exemplo 4
Num país distante, os números são escritos na base r e a moeda local é o *potiguar*, abreviada *Poti.* Um homem comprou um boi por 440 *potis*. Para efetuar a compra, ele deu ao vendedor uma cédula de 1000 *potis* e recebeu de troco 340 *potis*.
Qual é o valor da base r?
Solução

Pelos dados do problema, temos 1000 potis – 440 potis = 340 potis, na base r. Portanto,

$$(1.r^3 + 0.r^2 + 0.r + 0) – (4.r^2 + 4.r + 0) = 3.r^2 + 4.r + 0,$$

que é o mesmo que $r^3 – 7r^2 – 8r = 0$. Como a base r é um número positivo, podemos dividir ambos os lados por r, obtendo $r^2 – 7r – 8 = 0$. Resolvendo a equação, temos: $r = 8$ ou $r = -1$. Como a base r é positiva, r tem que ser igual a 8. Observe que, na base r, tem-se $440 + 340 = 1000$. Isso significa que $4 + 4 = 0$ no sistema de base r. Portanto, de fato, a base $r = 8$.

Exercício 4
O número natural K tem como representação na base 2 o número $111000110_{(2)}$. Qual é a representação binária do número M = 2.K?

Exemplo 5
O número 15! = 1 x 2 x 3 x ... x 14 x 15 (fatorial *de 15*) quando escrito na base decimal termina com a zeros. Quando escrevemos 15! na base 12, termina com b zeros.
Qual é o valor de $a.b$?
Solução

O que produz um zero no final de um número na base 10 é um fator de 10. Ou seja, a representação de um número natural M na base 10 termina com um único zero se M = 10 x K, onde K é um número natural e 10 não divide K. De modo análogo, a representação de um número natural Q na base 10 termina com dois zeros se $Q = 10^2$ x J, onde J é um número natural e 10 não divide J. Usando o raciocínio acima, a representação de 15! na base 10 termina com quantos zeros quantos forem seus fatores de 10. Mas,

15! = 1 x 2 x 3 x ... x 14 x 15 = 1 x **2** x 3 x 4 x **5** x 6 x 7 x **8** x 9 x **10** x 11 x 12 x 13 x 14 x **15** =
= (**2** x **5** x **10** x **2** x **5**) x (1 x 3 x 4 x 6 x 7 x 4 x 9 x 11 x 12 x 13 x 14 x 3) =
= $\mathbf{10^3}$ x (1 x 3 x 4 x 6 x 7 x 4 x 9 x 11 x 12 x 13 x 14 x 3).

Portanto, $a = 3$.

De modo análogo ao que fizemos acima, podemos concluir que: o que produz um zero no final de um número na base 12 é um fator de 12. Ou seja, a representação de um número natural M na base 12 termina com um único zero se M = 12 x K, K é um número natural e 12 não divide K. De modo análogo, a representação de um número natural Q termina com dois zeros se $Q = 12^2$ x J, onde J é um número natural e 12 não divide J. Assim, a representação de 15! na base 12 termina com quantos zeros quantos forem seus fatores de 12. Mas,

15! = 1 x 2 x 3 x ... x 14 x 15 = 1 x **2** x **3** x **4** x 5 x **6** x 7 x **8** x 9 x 10 x 11 x **12** x 13 x **14** x **15** =
= (**2** x **6** x **3** x **4** x **12** x **4** x **3** x **2** x **3** x **2**) x (1 x 5 x 7 x 3 x 10 x 11 x 13 x 7 x 5) =
= $\mathbf{12^5}$ x (1 x 5 x 7 x 2 x 3 x 10 x 11 x 13 x 7x 5).

Portanto, $b = 5$. Logo, $a.b = 3 \times 5 = 15$.

Exemplo 6
Um número K tem três dígitos na sua representação na base 7. Quando representamos K na base 9 os dígitos são os mesmos da representação na base 7 só que invertidos. Qual é a representação de K na base 10?
Solução

Sejam *a, b* e *c* os dígitos de K. Ou seja,

$$K = a \times 7^2 + b \times 7 + c = c \times 9^2 + b \times 9 + a .$$

Assim, temos: $b \times 7 - b \times 9 = (c \times 9^2 + a) - (a \times 7^2 + c)$, que é o mesmo que

$$-2b = 80c - 48a \text{ , ou seja } b = 24a - 40c = 8(3a - 5c).$$

Concluímos que o dígito *b* é um múltiplo de 8. Por outro lado, o dígito b satisfaz as desigualdades $0 \leq b < 7$. Logo, necessariamente temos $3a - 5c = 0$. Portanto, $b = 0$. Como $3a = 5c$, segue que *c* é divisível por 3 e 5 divide *a*. Mas, na base 7, K tem três dígitos. Portanto, *a* não pode ser zero e satisfaz as desigualdades $0 < a < 7$. Logo, $a = 5$ e $c = 3$. Concluímos que
$K = 503_{(7)} = 305_{(9)} = 248$ na base 10.

Exercício 5
Se o número $46_{(b)}$ é igual ao triplo de $15_{(b)}$, qual é o valor de b?

Exemplo 7 – O adivinho indiscreto
Convide um colega para dizer, dentre os 6 cartões abaixo, de 32 números cada, em quais deles está a sua idade. Imediatamente você advinha à idade dele.
Onde está o segredo?

1		2		4		8		16		32	
3	3	3	3	5	3	9	4	1	49	3	4
	5		5		7		1	7		3	9
5	3	6	3	6	3	1	4	1	50	3	5
	7		8		8	0	2	8		4	0
7	3	7	3	7	3	1	4	1	51	3	5
	9		9		9	1	3	9		5	1
9	4	1	4	12	4	1	4	2	52	3	5
	1	0	2		4	2	4	0		6	2
1	4	1	4	13	4	1	4	2	53	3	5
1	3	1	3		5	3	5	1		7	3
1	4	1	4	14	4	1	4	2	54	3	5
3	5	4	6		6	4	6	2		8	4
1	4	1	4	15	4	1	4	2	55	3	5
5	7	5	7		7	5	7	3		9	5
1	4	1	5	20	5	2	5	2	56	4	5
7	9	8	0		2	4	6	4		0	6
1	5	1	5	21	5	2	5	2	57	4	5
9	1	9	1		3	5	7	5		1	7
2	5	2	5	22	5	2	5	2	58	4	5
1	3	2	4		4	6	8	6		2	8
2	5	2	5	23	5	2	5	2	59	4	5
3	5	3	5		5	7	9	7		3	9
2	5	2	5	28	6	2	6	2	60	4	6
5	7	6	8		0	8	0	8		4	0
2	5	2	5	29	6	2	6	2	61	4	6
7	9	7	9		1	9	1	9		5	1
2	6	3	6	30	6	3	6	3	62	4	6
9	1	0	2		2	0	2	0		6	2
3	6	3	6	31	6	3	6	3	63	4	6
1	3	1	3		3	1	3	1		7	3
3		3		36		4		4		4	
3		4				0		8		8	

Solução

Um número natural K, entre 1 e 63, pode ser escrito na base 2 como

$$K = a_5 .2^5 + a_4 .2^4 + a_3.2^3 + a_2.2^2 + a_1.2 + a_0 ,$$

com cada um dos números a_5 , a_4 , a_3 , a_2 , a_1 , a_0 sendo 0 ou 1. Nesse caso, a representação do número K na base 2 é, exatamente, $a_5\, a_4\, a_3\, a_2\, a_1\, a_0$, onde $a_i = 0$ ou 1, i = 1,2,3,4,5.

Pois bem, na primeira lista do adivinho estão os números para os quais $a_0 = 1$, isto é, aqueles que terminam em 1 quando escritos na base 2; na segunda lista, estão os números para os quais $a_1 = 1$, ou seja, aqueles, entre 1 e 63, que têm 1 na segunda casa da direita para esquerda, quando escritos na base 2; na terceira, estão aqueles para os quais $a_2 = 1$ e assim por diante.
Fica claro, agora, porque cada idade é igual à soma dos primeiros números de cada lista em que ela esteja!

Exemplo 8
Uma base de numeração fatorial é aquela pela qual se expressaria um número inteiro positivo K como sendo:

$$K = a_1 + a_2 \,.\, 2! + a_3 \,.\, 3! + a_4 \,.\, 4! + ... + a_n \,.\, n!, \qquad (*)$$

onde $a_1, a_2, a_3, a_4, ..., a_n$ são inteiros não negativos com $0 \leq a_k \leq K$.
Expresse os seguintes números na base de numeração fatorial:
a) 7 b) 15 c) 85 d) 695
Solução

a) Observe que, como 4! = 24 > 7, só podemos expressar 7 como uma expressão do tipo $a_1 + a_2 \,.\, 2! + a_3 \,.\, 3!$. É fácil ver que $7 = 1 + 0 \,.\, 2! + 1.\, 3!$
b) Veja que 4! = 24 > 15. Logo a expressão para 15 na base fatorial deve ser do tipo $a_1 + a_2 \,.\, 2! + a_3 \,.\, 3!$. É fácil ver que $15 = 1 + 1 \,.\, 2! + 2.\, 3!$
c) Observe que 5! = 120 > 85. Logo, $85 = a_1 + a_2 \,.\, 2! + a_3 \,.\, 3! + a_4 \,.\, 4!$. Agora, é fácil ver que $85 = 1 + 0 \,.\, 2! + 2 \,.\, 3! + 3 \,.\, 4!$
d) Como 6! = 720, a expressão para 695 é do tipo $a_1 + a_2 \,.\, 2! + a_3 \,.\, 3! + a_4 \,.\, 4! + a_5 \,.\, 5!$. Agora, observe que $a_5 = 5$, caso contrário não atingiremos 695 e a_4 não pode ser 4, pois $4 \,.\, 4! + 5 \,.\, 5! > 695$. Por outro lado, a_4 não pode ser menor do que 3, pois se $a_4 = 2$, teremos $1 + 2 \,.\, 2! + 3 \,.\, 3! + 2 \,.\, 4! < 95$ e não conseguiríamos atingir 695. Logo, $a_4 = 3$. Agora, é fácil ver que $695 = 1 + 2 \,.\, 2! + 3 \,.\, 3! + 3 \,.\, 4! + 5 \,.\, 5!$.

Critérios de divisibilidade

Olhando somente para os números na base 10, temos vários critérios de divisibilidade. Ou seja, testes para saber se um número natural é divisível por outro sem ser preciso efetuar a divisão. Esse estudo será mais completo com a noção de congruência, a ser estudada na próxima aula. Como essa noção não é normalmente estudada no Ensino Médio, pretendemos adiantar alguns critérios de divisibilidade que possam ser provados facilmente sem o uso do conceito de congruências. Assim, a seguir vamos estudar os critérios de divisibilidade mais comuns.

a) Divisibilidade por 2

Um número natural K é divisível por 2 se, e só se, na sua representação na base 10, seu algarismo das unidades é divisível por 2. Ou seja, um número natural K é divisível por 2 se, e somente se, na sua representação na base 10, termina em 0, 2, 4, 6 ou 8.

De fato, representemos K na base 10 por:

$$K = c_n 10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2 10^2 + c_1 10 + c_0,$$

com $c_n, c_{n-1}, ..., c_3, c_2, c_1, c_0$ inteiros não negativos, todos menores do que 10 e c_0 sendo o dígito da unidades.
Se K é divisível por 2, então, explicitamos o valor de c_0 como sendo

$$c_0 = K - (c_n 10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2 10^2 + c_1 10).$$

Agora, observe que o número natural

$$(c_n 10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2 10^2 + c_1 10)$$

é divisível por 2 porque é uma soma de números pares. Logo, c_0 é divisível por 2, como diferença de dois números divisíveis por 2.
Se c_0 é divisível por 2, nesse caso,
$K = c_n 10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2 10^2 + c_1 10 + c_0$, é divisível por 2, pois é uma soma finita de números divisíveis por 2.

b) Divisibilidade por 3

Um número natural K é divisível por 3 se, e somente se, na sua representação na base 10, a soma de seus dígitos é um número divisível por 3.

De fato, representemos K na base 10 por:

$$K = c_n 10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2 10^2 + c_1 10 + c_0,$$

com $c_n, c_{n-1}, ..., c_3, c_2, c_1, c_0$ inteiros não negativos, todos menores do que 10. Agora, observe que: $10 = 9 + 1$ e $10^k = (9 + 1)^k$. Usando o desenvolvimento do Binômio de Newton para $(9 + 1)^k$, temos que $(9 + 1)^k = 9m_k + 1$, onde m_k é um número inteiro. Assim, temos que: $c_k 10^k = c_k(9 + 1)^k = c_k(9m_k + 1) = 9m_k c_k + c_k$. Logo,

$$\begin{aligned} K &= c_n 10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2 10^2 + c_1 10 + c_0 = \\ &= c_0 + (c_1 9m_1 + c_1)10 + (c_2 9m_2 + c_2) + (c_3 9m_3 + c_3) + ... + (c_n 9c_n + c_n) = \\ &= (c_1 9m_1 + c_2 9m_2 + c_3 9m_3 + ... + c_n 9c_n) + (c_0 + c_1 + c_2 + c_3 + ... + c_n) = \\ &= 9(c_1 m_1 + c_2 m_2 + c_3 m_3 + ... + c_n c_n) + (c_0 + c_1 + c_2 + c_3 + ... + c_n). \end{aligned}$$

Suponha que K seja divisível por 3. Como

$$(c_0 + c_1 + c_2 + c_3 + ... + c_n) = K - 9(c_1 m_1 + c_2 m_2 + c_3 m_3 + ... + c_n c_n),$$

segue que $(c_0 + c_1 + c_2 + c_3 + ... + c_n)$ é divisível por 3, por ser a diferença de dois números divisíveis por 3.

Por outro lado, se $(c_0 + c_1 + c_2 + c_3 + ... + c_n)$ é divisível por 3, segue que

$K = 9(c_1 m_1 + c_2 m_2 + c_3 m_3 + ... + c_n c_n) + (c_0 + c_1 + c_2 + c_3 + ... + c_n)$ é divisível por 3, como soma de dois números divisíveis por 3.

Exemplo 9
Verifique, sem efetuar a divisão, se o número 187134574 é divisível por 3.
Solução

Basta calcular a soma 1 + 8 + 7 + 3 + 4 + 5 + 7 + 4 = 41. Como 41 não é divisível por 3, concluímos que o número 187134574 não é divisível por 3.

Exemplo 10
Escreva a seqüência crescente de todos os números inteiros começados por 10 e terminados por 99 para formar o número inteiro

K = 10111213141516.....979899

Qual é a maior potência de 3 que divide K?
Solução

Observe que a soma 1 + 2 + 3 + ... + 9 = 45. Portanto, a soma dos dígitos do número K é igual: a soma dos números de 10 a 19 mais a soma dos números de 20 a 29, ..., soma dos números de 90 a 99, que é dada por :

(1 x 10 + 45) + (2 x 10 + 45) + (3 x 10 + 45) + (4 x 10 + 45) + ... + (9 x 10 + 45) =

= (1 + 2 + 3 + 4 + ... + 9) x 10 + 9 x 45 = 45 x 10 + 9 x 45 = 19 x 45 = 3^2 x 5 x 19.

Concluímos que o número é divisível por 9, pois na decomposição em fatores primos, o 3 comparece elevado ao quadrado.
Logo, a maior potência de 3 que divide K é dois.

c) Divisibilidade por 4

Um número natural K é divisível por 4 se, e somente se, na sua representação na base 10, o número formado pelos dois últimos dígitos (contados da esquerda para a direita) forma um número divisível por 4.

Observe que 4 = 04 e 8 = 08, ambos divisíveis por 4. Agora, suponha que K > 8 e a representação de K na base 10 seja:

$$K = c_n 10^n + c_{n-1} 10^{n-1} + ... + c_3 10^3 + c_2 10^2 + c_1 10 + c_0,$$

com $c_n, c_{n-1}, ..., c_3, c_2, c_1, c_0$ inteiros não negativos, todos menores do que 10.

Olhando para K como sendo K = $(c_n10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2\, 10^2)$+ $c_1 10 + c_0$, é fácil ver que a parcela $(c_n10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2\, 10^2) = 10^2(c_n10^{n-2} + c_{n-1}10^{n-3} + ... + c_3 10 + c_2)$ é divisível por 4, pois podemos escrever $10^2 = 4 \times 25$. Assim, é fácil concluir que K é divisível por 4 se, e só se, o número inteiro $c_1 10 + c_0$ é divisível por 4.

Exercício 6
Verifique, sem efetuar a divisão, se o número 2008 é divisível por 4.

d) Divisibilidade por 5

Um número natural K é divisível por 5 se, e só se, na sua representação na base 10, o dígito das unidades é zero ou cinco.

De fato, representemos K na base 10 por:

$$K = c_n10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2\, 10^2 + c_1 10 + c_0,$$

com $c_n, c_{n-1}, ..., c_3, c_2, c_1, c_0$ inteiros não negativos, todos menores do que 10 e c_0 sendo o dígito da unidades. Observe que a parcela $c_n10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2\, 10^2 + c_1 10$ é um número inteiro divisível por 5, pois é múltiplo de 10 e $10 = 2 \times 5$. Portanto, K é divisível por 5 se, e só se, c_0 é divisível por 5. Mas, $0 \le c_0 \le 9$. Logo, c_0 é 0 ou 5.

e) Divisibilidade por 6

Um número natural K é divisível por 6 se, e somente se, na sua representação na base 10, for divisível simultaneamente por 2 e por 3.

De fato, se K é divisível por 6, então, $K = 6k$, com k um número inteiro. Mas, podemos escrever $K = 6k = 2(3k) = 3(2k)$. Logo, K é múltiplo simultaneamente de 2 e 3.
Como 2 e 3 são primos, na decomposição em fatores primos do número K aparece o 2 e o 3. Logo, K é múltiplo do produto $2.3 = 6$.

f) Divisibilidade por 7

Antes de enunciar o critério de divisibilidade por 7, vamos fazer algumas considerações.
Seja K um número natural, cuja representação na base 10 é:

$$K = c_n10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2\, 10^2 + c_1 10 + c_0,$$

com $c_n, c_{n-1}, ..., c_3, c_2, c_1, c_0$ inteiros não negativos, todos menores que 10.

Agora, olhemos para a representação decimal de K como sendo a soma de duas parcelas:

$$K = c_n10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2\, 10^2 + c_1 10 + c_0, \text{ ou seja:}$$
$$K = 10(c_n10^{n-1} + c_{n-1}10^{n-2} + ... + c_3 10^2 + c_2\, 10 + c_1) + c_0$$

Chamando $M = c_n10^{n-1} + c_{n-1}10^{n-2} + ... + c_3 10^2 + c_2\, 10 + c_1$, podemos escrever K como sendo

$K = 10M + c_0$.

Enunciamos a seguir o teste de divisibilidade por 7.

Um número natural $K = 10M + c_0$ é divisível por 7 se, e somente se, o número natural $M + 5.c_0$ é divisível por 7.

De fato, se $K = 10M + c_0$ é divisível por 7, então, $5K = 5.(10M + c_0)$ também é divisível por 7. Mas, podemos escrever:

$$5K = 5.(10M + c_0) = 50M + 5.c_0 = 49M + M + 5.c_0.$$

Portanto, $M + 5.c_0 = 5K – 49M$ é um múltiplo de 7, como diferença de dois múltiplos de 7. Por outro lado, se $M + 5.c_0$ é um múltiplo de 7, então, $10(M + 5.c_0)$ é um múltiplo de 7. Mas,

$$10(M + 5.c_0) = 10M + 50c_0 = 49c_0 + (10M + c_0) = 49.c_0 + K.$$

Portanto, $K = 10(M + 5.c_0) - 49.c_0$ é um múltiplo de 7, pois é a diferença de dois múltiplos de 7.

Exemplo 11

Verifique, sem efetuar a divisão, se o número 1729 é divisível por 7.

Solução

Pelo que vimos anteriormente, escrevemos $K = 1729 = 9 + 10 \times (172)$ e K será divisível por 7 se, e somente se, o número $5 \times 9 + 172 = 217$ for divisível por 7.

Aplicando o critério para o número 217, temos que $217 = 7 + 10 \times (21)$ será divisível por 7 se, e somente se, o número $5 \times 7 + 21 = 56$ for divisível por 7.

Como 56 é divisível por 7, pois $56 = 7 \times 8$, concluímos que 217 é divisível por 7. Agora, observe que:

1729 é divisível por 7 $\Leftrightarrow$ 217 é divisível por 7 $\Leftrightarrow$ 56 é divisível por 7.

Portanto, 1729 é divisível por 7.

Exercício 7

Verifique, sem efetuar a divisão, se o número 23921083 é divisível por 7.

g) Divisibilidade por 8

Um número natural K é divisível por 8 se, e somente se, na sua representação na base 10, o número formado pelos três últimos dígitos (contados da esquerda para a direita) forma um número divisível por 8.

$$K = c_n 10^n + c_{n-1} 10^{n-1} + ... + c_3 10^3 + c_2 10^2 + c_1 10 + c_0,$$

com $c_n, c_{n-1}, ..., c_3, c_2, c_1, c_0$ inteiros não negativos, todos menores do que 10. Olhamos para K da seguinte maneira:

$K = 10^3(c_n 10^{n-3} + c_{n-1}10^{n-4} + ... + c_3 10) + c_2 10^2 + c_1 10 + c_0$

Agora, é fácil ver que a parcela $10^3(c_n 10^{n-3} + c_{n-1}10^{n-4} + ... + c_3 10)$ é divisível por 8, pois $10^3 = 1000 = 8 \times 125$. Portanto, é fácil ver que N é divisível por 8 se, e só se, o número

$c_2\, c_1 c_0 = c_2 10^2 + c_1 10 + c_0$ é um número divisível por 8.

A justificativa é a mesma feita para o caso da divisibilidade por 2 e 4.

h) Divisibilidade por 9

Um número natural K é divisível por 9 se, e somente se, na sua representação na base 10, a soma de seus dígitos é um número divisível por 9.

A justificativa é a mesma feita para o caso da divisibilidade por 3.

i) Divisibilidade por 10

Um número natural K é divisível por 10 se, e somente se, na sua representação na base 10, é divisível simultaneamente por 2 e por 5. Ou, que é o mesmo: um número natural K é divisível por 10 se, e somente se, na sua representação na base 10, o algarismo das unidades é zero.

A justificativa é a mesma feita para o caso da divisibilidade por 6, mudando os primos 2 e 3 para 2 e 5.

j) Divisibilidade por 11

Um número natural K é divisível por 11 se, e somente se, na sua representação na base 10, a soma de seus dígitos nas posições pares menos a soma dos dígitos nas posições ímpares é um número divisível por 11.

De fato, representemos K na base 10 por:

$K = c_n 10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2 10^2 + c_1 10 + c_0,$

com $c_n, c_{n-1}, ..., c_3, c_2, c_1, c_0$ inteiros não negativos, todos menores que 10.
Agora, observe que: $10 = 11 - 1$ e $10^k = (11 - 1)^k$. Usando o desenvolvimento do Binômio de Newton para $(11 - 1)^k$, temos que:

$(11 - 1)^k = 11m_k + 1$, se k é um inteiro par e m_k é um número inteiro e
$(11 - 1)^k = 11m_k - 1$, se k é um inteiro ímpar e m_k é um número inteiro.

Assim, temos que:

$c_k 10^k = c_k(11 - 1)^k = c_k(11m_k + 1) = 11m_k c_k + c_k$, se k é um inteiro par e
$c_k 10^k = c_k(11 - 1)^k = c_k(11m_k - 1) = 11m_k c_k - c_k$, se k é um inteiro ímpar.

Portanto, temos que

$K = c_0 + c_1 10 + c_2 10^2 + c_3 10^3 + ... + c_n 10^n =$
$= c_0 + 11m_1c_1 - c_1 + 11m_2c_2 + c_2 + 11m_3c_3 - c_3 + 11m_4c_4 + c_4 + ... + 11m_nc_n + (-1)^k c_n,$
$= (c_0 - c_1 + c_2 - c_3 + c_4 - .....+ (-1)^k c_n) + (11m_1c_1 + 11 m_2c_2 + 11m_3c_3 + 11 m_4c_4 + 11m_nc_n)$
$= (c_0 - c_1 + c_2 - c_3 + c_4 - .....+ (-1)^k c_n) + 11s,$ com $s \in \mathbf{Z}$.

Portanto, é fácil ver que K é divisível por 11 se, e somente se, $(c_0 - c_1 + c_2 - c_3 + c_4 - .....+ (-1)^k c_n)$ é divisível por 11.

Exemplo 12
Verifique, sem efetuar a divisão, se o número 90806375 é divisível por 11.

Solução

Basta calcular a soma $9 - 0 + 8 - 0 + 6 - 3 + 7 - 5 = 22$, que é divisível por 11. Logo, o número 90806375 é divisível por 11.

Exercício 8
Verifique, sem efetuar a divisão, se o número 28382607 é divisível por 11.

Exemplo 13
Considere a sequência de números inteiros dada por

1, 2, 2, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5, 6, 6, 6, 6, 6, 6, ...

na qual o n-ésimo número inteiro positivo aparece n vezes.

Qual é o termo de ordem 2007?
Solução

Observe que o 1 só aparece uma vez e na posição 1. A última aparição do segundo inteiro, 2, é na terceira posição: $1 + 2 = 3$.
A última aparição do 3 é na sexta posição: $1 + 2 + 3 = 6$.
A última aparição do 4 é na sexta posição: $1 + 2 + 3 + 4 = 10$.
É fácil ver que a última aparição do n-ésimo número inteiro positivo é na sexta posição:

$1 + 2 + 3 + 4 + ... + n = n(n+1)/2.$

Observe agora que: $(62 \times 63)/2 = 1953 < 2007$ e $(63 \times 64)/2 = 2016 > 2007$. Isso significa que a última aparição de 62 na sequência é na posição de número 1953 e que a última posição de 63 é a de número 2016. Portanto, o termo de ordem 2007 é 63.

Exercícios

1) Escreva na base 7 o número cuja representação na base 5 é $14432_{(5)}$.

2) Escreva os primeiros 25 inteiros positivos na base 12.

3) Encontre o dígito das unidades do número

(a) 107^{2007} (b) 24^{100} (c) $1 + 2 + 3 + \ldots + 100$

4) Ana, uma adolescente, tem o quadrado da idade dela igual ao número da casa, na rua em que mora. A idade dela e o número da casa têm o mesmo dígito das unidades, mas a soma desses números não é um múltiplo de 10.
Qual é a idade de Ana?

5) Se o número $81_{(b)}$ é igual ao triplo de $15_{(b)}$, qual é o valor de b?

6) Qual é o maior número de três dígitos na base 14?

7) Encontre os números naturais a e b tais que: $1727 = a.8^3 + b$, onde $0 \leq b < 8^3$.

8) Verifique que: quando se subtrai de um número natural, na sua representação na base 10, a soma de seus dígitos, o resultado é um número divisível por 9.

9) Verifique, sem efetuar a divisão, se o número 174557974 é divisível por 7.

10) Na sua representação na base 10, quantos dígitos tem o número 7×5^{41}?

Sugestão – Seja $K = 7 \times 5^{41}$. Verifique que o logaritmo na base 10 de K é, aproximadamente, igual 29,5.

11) Teste de Divisibilidade por 13 – Dê uma justificativa para o teste de divisibilidade por 13, apresentado abaixo.

Seja K um número natural, cuja representação na base 10 é:

$$c_n 10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2 10^2 + c_1 10 + c_0,$$

com $c_n, c_{n-1}, ..., c_3, c_2, c_1, c_0$ inteiros não negativos, todos menores que 10.
Agora, olhemos para a representação decimal de K como sendo a soma de duas parcelas:

$K = (c_n 10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2 10^2 + c_1 10) + c_0$, ou seja:

$K = 10(c_n 10^{n-1} + c_{n-1}10^{n-2} + ... + c_3 10^2 + c_2 10^1 + c_1) + c_0$.

Chamando $M = c_n 10^{n-1} + c_{n-1}10^{n-2} + ... + c_3 10^2 + c_2 10^1 + c_1$, *podemos escrever K como sendo*

$$K = 10M + c_0.$$

Um número natural K é divisível por 13 se, e somente se, o número natural $M + 4.c_0$ é divisível por 13.

12) Encontre o maior número primo (escrito na base 10) que divide a soma:

$$1_2 + 10_2 + 100_2 + 1000_2 + \ldots + 100000000_2.$$

13) Reduza a fração $\frac{116.690.151}{427.863.887}$ na sua forma mais simples.

14) Mostre que o $(1110).(1111).(1112).(1113) = (1.235.431)^2 - 1$ em qualquer sistema de numeração de base maior do que 5.

15) Em que base b o número $M = 11111_b$ é um quadrado perfeito?

16) Um juiz resolve dar uma chance de liberdade para um condenado à morte. O condenado tem que adivinhar uma senha que o livrará da sentença de morte. A senha é formada por três números distintos, x, y e z, de dois dígitos cada um. O condenado tem de identificar três números A, B e C, de tal modo que permita encontrar o número $Ax + By + Cz$ fornecido pelo juiz e daí encontrar a senha x, y e z.

Como você pode ajudar o condenado a obter a liberdade?

Sugestão – O condenado tem que descobrir um método para distinguir os três números de dois dígitos. A base 100 é a saída. Escreva $A = 100^2$, $B = 100$ e $C = 1$ e $Ax + By + Cz = x.100^2 + y.100 + z.1$.

Resumo

Nesta aula, estudamos a representação dos números naturais numa base qualquer e os critérios de divisibilidade, que em alguns casos nos permitem decidir se um determinado inteiro é ou não divisível por outro, sem precisar efetuar a divisão.

Referências

BURTON, David M. **Elementary number theory**. New York: McGraw-Hill, 1998.

COUTINHO, S. C. **Números inteiros e criptografia RSA**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada – IMPA/ Sociedade Brasileira de Matemática – SBM, 1997.

CRAWFORD, Mathew. **Introduction number theory**: the art of problem solving. Alphine: AoPS Incorporated, 2006.

EARL, M. James; SALKIND, Charles T. **The contest problem book III**. Washington: The Mathematical Association of American, 1973.

HEFEZ, Abramo. **Elementos de aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2005.

SALKIND, Charles T. **The contest problem book II**. Washington: The Mathematical Association of American, 1966

Aula 7 – Congruências

Apresentação

Nesta aula, estudaremos o conceito de **congruência,** que revolucionou o estudo da Aritmética, permitindo tratar as questões de divisibilidade com um enfoque mais fácil e mais eficiente. Foi Carl Friederich Gauss (1777- 1855) quem introduziu este conceito, em 1801, no seu livro Disquisitiones aritmeticae (Investigações na Aritmética). Gauss escreveu este livro quando ele tinha apenas 24 anos.

Tente entender tudo que está sendo explicado na aula. Estude com caneta e papel ao lado. Leia com atenção. Se for preciso, leia várias vezes uma linha ou um parágrafo. Seja paciente e procure ter certeza que você entendeu o que (e por que) está fazendo.

Objetivos

- Decidir quando dois números são congruentes.
- Aplicar corretamente as propriedades de congruência.
- Decidir se um dado número inteiro positivo divide outro número inteiro, usando propriedades das congruências
- Resolver congruências lineares.

A definição de congruência

Dados os números inteiros 33, 18 e 3, temos que 33 – 18 = 15 = 3 x 5. Portanto, a diferença 33 – 18 é divisível por 3. Dizemos então que 33 é côngruo a 18 módulo 3.

Johann Carl Friedrich Gauss (1777-1855), conhecido como Gauss, famoso matemático, astrônomo e físico alemão, sugeriu uma notação para esse fato, a qual ficou mundialmente aceita:

$33 \equiv 18 \pmod 3 \Leftrightarrow 33 - 18$ é divisível por 3.

Lê-se: 33 é côngruo a 18 módulo 3 se, e somente se, a diferença 33 – 18 é divisível por 3. De um modo equivalente, escrevemos:

$33 \equiv 18 \pmod 3 \Leftrightarrow 33 - 18 = 3k$, com $k \in \mathbf{Z}$.

Dizemos, também, que 33 e 18 são côngruos entre si módulo *3*.

Vejamos outro exemplo: 27 e 13 são côngruos módulo 7 (e também côngruos módulo 2), pois a diferença 27 – 13 = 14 = 2 x 7. Ou seja, $13 \equiv 27 \pmod 7$ e $13 \equiv 27 \pmod 2$. É fácil ver que:

$18 \equiv -1 \pmod{19}$;

$31 \equiv 1 \pmod 2$;
$-3 \equiv 4 \pmod 7$;
$12 \equiv 0 \pmod 3$.

Exemplo 1
Mostre que quaisquer dois números inteiros pares são côngruos entre si módulo 2.

Solução

Sejam $2m$ e $2n$ dois números pares. A diferença $2m - 2n = 2.(m - n)$. Portanto, divisível por 2. Na notação de Gauss: $2m \equiv 2n \pmod 2$, para quaisquer m e n inteiros.

Exercício 1
Mostre que quaisquer dois números inteiros **ímpares** são côngruos entre si módulo 2.

De uma maneira geral, se a e b são dois números inteiros quaisquer e n é um número inteiro maior do que ou igual a 2, dizemos que a é côngruo a b módulo n se a – b = nk, com k um número inteiro. Na notação de Gauss:

$a \equiv b \pmod n \Leftrightarrow a - b = nk$, com k um número inteiro.

Uma propriedade muito útil, que decorre imediatamente da definição de congruência, é a seguinte:

Proposição 1
Dizer que a ≡ b (mod n) é equivalente a dizer que a e b deixam o mesmo resto na divisão por n.
Demonstração

Se $a \equiv b \pmod n$, então, $a - b = n$.k, onde k é um inteiro. Fazendo a divisão de a e b por n, temos:

$a = q_1.n + r_1$, onde q_1 e r_1 são números inteiros, com $0 \leq r_1 < n$,
$b = q_2.n + r_2$, onde q_2 e r_2 são números inteiros, com $0 \leq r_2 < n$.

Suponha que $r_2 \leq r_1$. Nesse caso, $0 \leq r_1 - r_2 \leq r_1 <$ n. Agora, fazemos a diferença:
$a - b = (q_1 - q_2)n + (r_1 - r_2)$ (*)

Desse modo, $0 \leq r_1 - r_2 <$ n é o resto da divisão de $a - b$ por n. Logo, $r_1 - r_2 = 0$, pois $a - b$ é múltiplo de n.

Reciprocamente, se a e b deixam o mesmo resto na divisão por n, então:

$a = q_1.n + r$, onde q_1 e r são números inteiros, com $0 \leq r < n$,
$b = q_2.n + r$, onde q_1 e r são números inteiros, com $0 \leq r < n$.

Daí, segue que $a - b = (q_1 - q_2)n$. Portanto, a diferença $a - b$ é um múltiplo de n, o que equivale a dizer que $a \equiv b \pmod n$.

Quando dois números, a e b, não são côngruos (ou não são congruentes) módulo n, dizemos que a e b são incongruentes (ou incôngruos) módulo n.

Propriedades básicas das congruências

Se a, b, c e d são inteiros quaisquer e n é um inteiro maior do que ou igual a 2, são verdadeiras as seguintes propriedades:

I. $a \equiv a \pmod{n}$ (Reflexividade)
II. Se $a \equiv b \pmod{n}$, então $b \equiv a \pmod{n}$ (Simetria)
III. Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então, $a \equiv c \pmod{n}$ *(Transitividade)*
IV. Se $a \equiv b \pmod{n}$ *e* $c \equiv d \pmod{n}$, *então,* $a + c \equiv b + d \pmod{n}$ *(Soma)*
V. *Se* $a \equiv b \pmod{n}$ *e* $c \equiv d \pmod{n}$, *então,* $a - c \equiv b - d \pmod{n}$ (Diferença)
VI. *Se* $a \equiv b \pmod{n}$ e c é um inteiro não negativo, então, $ac \equiv bc \pmod{n}$
VII. *Se* $a \equiv b \pmod{n}$ *e* $c \equiv d \pmod{n}$, *então,* $a.c \equiv b.d \pmod{n}$ *(*Produto*)*
VIII. *Se* $a \equiv b \pmod{n}$ *e* k é um inteiro positivo, então, $a^k \equiv b^k \pmod{n}$ *(*Potência*)*
IX. *Se* $a + c \equiv b + c \pmod{n}$, então, $a \equiv b \pmod{n}$ (Cancelamento para a soma)

Você pode verificar facilmente que as propriedades anteriores são de fato verdadeiras.

Por exemplo, para verificar a veracidade da propriedade *IV*, temos que mostrar que a diferença $(a + c) - (b + d)$ é múltiplo de n. Para isso, basta observar que:

$$(a + c) - (b + d) = (a - b) + (c - d)$$

e *que* $(a - b)$ e $(c - d)$ são, por hipótese, ambos múltiplos de n. Logo, $(a + c) - (b + d)$ é um múltiplo de n, como soma de dois múltiplos de n. Portanto, $a + c \equiv b + d \pmod{n}$.

Para verificar a veracidade da propriedade *VII*, temos que mostrar que $a.c - b.d$ é um múltiplo de n. Para isso, basta observar que:

$$a.c - b.d = a.c \mathbf{- b.c + b.c} - b.d = (a - b).c + b.(c - d).$$

Como $(a - b)$ e $(c - d)$ são, por hipótese, ambos múltiplos de n, segue que cada uma das duas parcelas, $(a - b).c$ e $b.(c - d)$, são múltiplos de n. Assim, $a.c - b.d$ é um múltiplo de n. Portanto, $a.c \equiv b.d \pmod{n}$.

Para verificar a propriedade *VIII*, basta aplicar a propriedade *VII* usando a congruência $a \equiv b \pmod{n}$ k vezes.

A propriedade *IX*, de fácil verificação, é o cancelamento para a soma. Exemplificando, como $15 + 4 \equiv 9 + 4 \pmod{6}$, segue que $15 \equiv 9 \pmod{6}$.

Exemplo 2

Ana, Bernardo e Carla arrumam laranjas para vender na feira, colocando 12 laranjas em cada saco. Ana tinha 389 laranjas, Bernardo 188 e Carla 97. Depois de arrumar todas as laranjas nos sacos, quantas sobraram ao todo?

Solução

Para responder, temos que observar que precisamos considerar, para cada um deles, a quantidade de laranjas módulo 12. Como $389 \equiv 5 \pmod{12}$; $188 \equiv 8 \pmod{12}$ e $97 \equiv 1 \pmod{12}$, quando Ana terminou de arrumar as laranjas nos sacos, sobraram 5 laranjas, das laranjas de Bernardo sobraram 5 e das de Carla sobrou 1. Portanto, no final sobraram $5 + 8 + 1 = 14$ laranjas. Mas, $14 \equiv 2 \pmod{12}$. Isso significa que eles, em conjunto, poderiam completar mais um saco com 12 laranjas e sobrariam apenas 2 laranjas.

Exercício 2

Encontre todos os inteiros n tal que $-100 \leq n \leq 100$, e $n \equiv 7 \pmod{19}$.

Exemplo 3

Sejam a, b e c números inteiros positivos cujos restos na divisão por 8 são 3, 5 e 1, respectivamente.

Ache o resto da divisão de $(a + b + c)$ por 8.

Solução

Temos que $a \equiv 3 \pmod{8}$, $b \equiv 5 \pmod{8}$ e $c \equiv 1 \pmod{8}$. Somando membro a membro as três congruências, obtemos $(a + b + c) \equiv 3 + 5 + 1 \pmod{8}$. Ou seja,
$(a + b + c) \equiv 9 \pmod{8}$. Como $9 \equiv 1 \pmod{8}$, segue que $(a + b + c) \equiv 1 \pmod{8}$.

Uma pergunta: nas congruências, vale o cancelamento para o produto?

Ou seja, se $ac \equiv bc \pmod{n}$, então, $a \equiv b \pmod{n}$?

Resposta: é fácil obter exemplos onde **não** se verifica a propriedade. Por exemplo, $3 \times 23 \equiv 3 \times 8 \pmod{9}$ é verdadeiro, enquanto $23 \equiv 8 \pmod{9}$ **não é verdadeiro,** pois $23 - 8 = 15$, que não é divisível por 9.

Conclusão: de uma maneira geral, **não** podemos aplicar o cancelamento numa situação como $ac \equiv bc \pmod{n}$, para obter $a \equiv b \pmod{n}$. O resultado correto seria:

Proposição 2

Se $ac \equiv bc \pmod{n}$, então, $a \equiv b \pmod{n/d}$, onde $d = MDC(c, n)$.

Demonstração

Se $ac \equiv bc \pmod{n}$, existe um inteiro k tal que $ac - bc = kn$.

*Agora, s*eja $d = \text{MDC}(c, n)$. Dividindo por d ambos os lados da igualdade $ac - bc = kn$, obtemos $(a - b)(c/d) = k(n/d)$. Por outro lado, como $d = \text{MDC}(c, n)$, existem números inteiros x e y tais que $cx + ny = 1$. Logo, $\frac{c}{d}x + \frac{n}{d}y = 1$. Pelo Corolário 2, da

aula 5 – O máximo divisor comum, o mínimo múltiplo comum e as equações diofantinas lineares –, segue que $\frac{c}{d}$ *e* $\frac{n}{d}$ são primos entre si.

Como MDC (*c/d, n/d*) = 1, então, *n/d* divide *a – b*, que é o mesmo que dizer $a \equiv b \ (mod \ \frac{n}{d})$.

Corolário

Seja $ac \equiv bc \ (mod \ n)$. Se *c* e *n* são primos entre si, então, $a \equiv b \ (mod \ n)$. Isto é, nessas hipóteses vale a lei do cancelamento para o produto.

Demonstração

Se *a* e *n* são primos entre si, então, MDC(*n*, *c*) = 1. Logo, $\frac{n}{MDC(n,c)} = \frac{n}{\mathbf{1}} = n$.

Exemplo 4

Verifique que 3 x 23 ≡ 3 x 8 (mod 9) implica que 23 ≡ 8 (mod 3).

Solução

Aplicando a propriedade anterior para 3 x 23 ≡ 3 x 8 (mod 9), obtemos 23 ≡ 8 (mod 9/3). Ou seja, 3 x 23 ≡ 3 x 8 (mod 9) implica que 23 ≡ 8 (mod 3).

Exercício 2

Sejam *a* e *b* números inteiros tais que $4a \equiv 4b \ (mod \ 15)$.

Diga, justificando, se podemos concluir que $a \equiv b \ (mod \ 15)$.

A seguir, vamos fazer alguns exemplos com os quais você vai poder verificar como o uso do conceito de congruência facilita a resolução de certos problemas.

Exemplo 5

Sem efetuar a divisão, encontre o resto da divisão de 4^{100} por 5.

Solução

Como 4 – (-1) = 4 + 1 = 5, podemos dizer que $4 \equiv -1 \ (mod \ 5)$. Aplicando a propriedade *VIII*, tomando *k* = 100, temos $4^{100} \equiv (-1)^{100} \ (mod \ 5)$. Ou seja, $4^{100} \equiv 1 \ (mod \ 5)$. Portanto, o resto da divisão de 4^{100} por 5 é o mesmo resto da divisão de 1 por 5. Mas, o resto da divisão de 1 por 5 é 1, pois 1 = 0 x 5 + 1. Logo, o resto da divisão de 4^{100} por 5 é 1.

Exemplo 6

A distribuição dos dias do mês num calendário é um exemplo do uso do conceito de congruência. Vejamos o calendário do mês de setembro do ano de 2008:

Setembro de 2008

D	S	T	Q	Q	S	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Observe a segunda coluna, a das segundas-feiras, ela começa com o 1 e todos os outros números dessa coluna deixam resto 1 quando divididos por 7. A coluna da sexta-feira, começa com 5 e todos os outros números deixam resto 2 quando divididos por 7. Ou seja, em todas as colunas os números são côngruos entre si módulo 7.

Exercício 3
Encontre todos os inteiros n tal que: $100 \leq n \leq 200$, e $3n \equiv 7 \pmod{19}$.

Exercício 4
Descreva o modelo de congruência para um relógio de ponteiros.

Exemplo 7
Dado um inteiro qualquer n, podemos afirmar que o número $(n^2 + 1)$ **não** é divisível por 3.
Solução

De fato, na divisão de um número inteiro por 3, os possíveis restos são 0, 1 ou 2. Desse modo, acontece uma, e só uma, das seguintes possibilidades:

ou $n \equiv 0 \pmod 3$, ou $n \equiv 1 \pmod 3$, ou $n \equiv 2 \pmod 3$.

Se $n \equiv 0 \pmod 3$, então, $n^2 \equiv 0 \pmod 3$, aplicando a propriedade *VIII*. Daí, segue que $n^2 + 1 \equiv 1 \pmod 3$. Portanto, nesse caso, $n^2 + 1$ deixa resto 1 quando dividido por 3.
Se $n \equiv 1 \pmod 3$, então, $n^2 + 1 \equiv 2 \pmod 3$. Nesse caso, $n^2 + 1$ deixa resto 2 quando dividido por 3.
Se $n \equiv 2 \pmod 3$, então, $n^2 \equiv 2^2 \pmod 3$, que é o mesmo que $n^2 \equiv 1 \pmod 3$. Logo, podemos dizer que $n^2 + 1 \equiv 2 \pmod 3$. Nesse caso, na divisão por 3 o número $n^2 + 1$ deixa resto 1. Portanto, para todo n, $n^2 + 1$ não é divisível por 3.

Exemplo 8
Diga, justificando, se o número $30^{99} + 61^{100}$ é um número divisível por 31.

Solução
Observe que $30 \equiv -1 \pmod{31}$. Portanto, $30^{99} \equiv (-1)^{99} \pmod{31}$. Logo, $30^{99} \equiv -1 \pmod{31}$. Por outro lado, $61 \equiv -1 \pmod{31}$. Portanto, $61^{100} \equiv (-1)^{100} \pmod{31}$. Logo, $61^{100} \equiv 1 \pmod{31}$. Assim, $30^{99} + 61^{100} \equiv -1 + 1 \pmod{31}$, que é o mesmo que $30^{99} + 61^{100} \equiv 0 \pmod{31}$. Portanto, $30^{99} + 61^{100}$ é um número divisível por 31.

Exemplo 9
Mostre que o número $43^{101} + 23^{101}$ é divisível por 66.

Solução

De fato, como $66 = 6 \times 11$, então, um número é divisível por 66 se, e somente se, é divisível simultaneamente por 6 e 11. Agora, $43 \equiv 1 \pmod 6$ e $23 \equiv -1 \pmod 6$. Portanto, usando propriedades básicas das congruências, podemos dizer que: $43^{101} \equiv 1 \pmod 6$ e $23^{101} \equiv -1 \pmod 6$. Somando ambas as congruências, obtemos $43^{101} + 23^{101} \equiv 1 + (-1) \pmod 6$, que é o mesmo que $43^{101} + 23^{101} \equiv 0 \pmod 6$. Assim, $43^{101} + 23^{101}$ é divisível por 6. Resta mostrar que $43^{101} + 23^{101}$ é divisível por 11. Para isso, observe que $43 \equiv -1 \pmod{11}$ e $23 \equiv 1 \pmod{11}$. Portanto, podemos dizer que $43^{101} \equiv -1 \pmod{11}$ e $23^{101} \equiv 1 \pmod{11}$. Logo, $43^{101} + 23^{101} \equiv 0 \pmod{11}$, que é o mesmo que dizer que $43^{101} + 23^{101}$ é divisível por 11. Portanto, como $43^{101} + 23^{101}$ é divisível simultaneamente por 6 e por 11, então, $43^{101} + 23^{101}$ é divisível por 66.

Exercício 5
Sejam a e n dois números inteiros.
Prove que: $(n - a)^2 \equiv a^2 \pmod n$.

Exemplo 10
Diga, justificando, se existe um número natural n tal que o número $(n^2 + n + 1)$ seja divisível por 55.
Solução

Inicialmente, observe que um número é divisível por 55 se ele o for por 5 e 11 ao mesmo tempo, pois $55 = 5 \times 11$. Por outro lado, dado um número natural n, uma e só uma das afirmações abaixo é verdadeira: ou $n \equiv 0 \pmod 5$ ou $n \equiv 1 \pmod 5$ ou $n \equiv 2 \pmod 5$ ou $n \equiv 3 \pmod 5$ ou $n \equiv 4 \pmod 5$. Agora, observe que:

se $n \equiv 0 \pmod 5$, então, $(n^2 + n + 1) \equiv 1 \pmod 5$;
se $n \equiv 1 \pmod 5$, então, $(n^2 + n + 1) \equiv 3 \pmod 5$;
se $n \equiv 2 \pmod 5$, então, $(n^2 + n + 1) \equiv 2 \pmod 5$;
se $n \equiv 3 \pmod 5$, então, $(n^2 + n + 1) \equiv 3 \pmod 5$;
se $n \equiv 4 \pmod 5$, então, $(n^2 + n + 1) \equiv 1 \pmod 5$.

Portanto, em nenhuma dos casos possíveis $(n^2 + n + 1) \equiv 0 \pmod 5$. Logo, não existe um número natural n tal que o número $(n^2 + n + 1)$ seja divisível por 55.

Exemplo 11
Ache o dígito das unidades do número 3^{100}.
Solução

Suponha que a representação decimal de 3^{100} seja $c_0 + c_1 10 + c_2 10^2 + c_3 10^3 + ... + c_n 10^n$, com $c_0, c_1, c_2, ..., c_n$ inteiros não negativos, todos menores do que 10. O que queremos encontrar é o valor de c_0. Na linguagem das congruências, $3^{100} \equiv c_0 \pmod{10}$. Agora, observe que $3^2 \equiv -1 \pmod{10}$. Logo, $3^{100} = (3^2)^{50} \equiv (-1)^{50} \pmod{10}$. Portanto, podemos escrever $3^{100} \equiv 1 \pmod{10}$. Assim, o dígito das unidades de 3^{100} é 1.

Exercício 6
Seja $A = 3^{105} + 4^{105}$.

(a) Mostre que 7 divide A. (b) Encontre o resto da divisão de A por 11.

Exemplo 12
Mostre que 7 divide o número $2222^{5555} + 5555^{2222}$.
Solução

É fácil ver que: $2222 \equiv 3 \pmod 7$, $5555 \equiv 4 \pmod 7$ e $3^5 \equiv 5 \pmod 7$. Usamos as propriedades básicas das congruências para escrever:

$2222^{5555} \equiv 3^{5555} \pmod 7$,
$5555^{2222} \equiv 4^{2222} \pmod 7$,
$3^{5555} = (3^5)^{1111} \equiv 5^{1111} \pmod 7$,
$4^{2222} = (4^2)^{1111} \equiv (-5)^{1111} \pmod 7 \equiv -\,5^{1111} \pmod 7$.

Portanto, $2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \pmod 7 \equiv 5^{1111} - 5^{1111} \pmod 7 \equiv 0 \pmod 7$.
Logo, 7 divide o número $2222^{5555} + 5555^{2222}$.

Exemplo 13
Encontre todos os quadrados módulo 13.
Solução

Pelo algoritmo da divisão, o resto da divisão de *n* por 13 varia de 0 a 12, como $n^2 \equiv (13 - n)^2 \pmod{13}$, só precisamos nos preocupar com os quadrados dos números não negativos de 0 até 6. Desse modo, $0^2 \equiv 0 \pmod{13}$;

$1^2 \equiv 1 \pmod{13}$;
$2^2 \equiv 4 \pmod{13}$;
$3^2 \equiv 9 \pmod{13}$;
$4^2 \equiv 3 \pmod{13}$;
$5^2 \equiv 12 \pmod{13}$;
$6^2 \equiv 10 \pmod{13}$.

Portanto, os quadrados módulo 13 são: 0, 1, 3, 4, 9, 10 e 12 .

Exemplo 14
Usando o conceito de congruência, demonstre que:
um número natural K é divisível por 9 se, e somente se, na sua representação na base 10, a soma de seus dígitos é um número divisível por 9.
Solução

Seja $K = c_n 10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2 10^2 + c_1 10 + c_0$, com $c_n, c_{n-1}, c_{n-2}, ..., c_0$ inteiros não negativos, todos menores do que 10, a representação de K na base 10. Agora observe que:
$10 \equiv 1 \pmod 9$ e $10^i \equiv 1 \pmod 9$. Dessa forma, temos que:

$K = c_n 10^n + c_{n-1}10^{n-1} + ... + c_3 10^3 + c_2 10^2 + c_1 10 + c_0 \equiv c_n + c_{n-1} + c_{n-2} + ... + c_0 \pmod 9$, o que demonstra a afirmação.

Exercício 7
Mostre que se $a^2 \equiv b^2 \pmod{p}$, onde p é um número primo, então, ou p divide $a + b$ ou p divide $a - b$.

Um sistema completo de restos módulo n é um conjunto com n números inteiros de tal forma que dois quaisquer deles **não** sejam congruentes módulo n.

Por exemplo, o conjunto S = {1, 2, 3, ..., n – 2, n – 1} é um sistema completo de resto módulo n.

Exemplo 15
Verifique que o conjunto {3, 13, 35} é um sistema completo de restos módulo 3.
Solução

Basta ver que $3 \equiv 0 \pmod{3}$, $13 \equiv 1 \pmod{3}$ e $35 \equiv 2 \pmod{3}$.

Exercício 8
Verifique que o conjunto S = {-14, 20, 22, 32, 47, 86, 143} é um sistema completo de restos módulo 7.

Congruências lineares

Uma congruência linear é uma equação da forma $ax \equiv b \pmod{n}$, onde a, b, n $\in$ Z , com n > 1. Uma solução de uma equação desse tipo é um inteiro x_o para o qual $ax_o \equiv b \pmod{n}$.

Agora, observe que $ax_o \equiv b \pmod{n}$ se, e somente se, n divide $ax_o - b$. Ou seja,

$$\boldsymbol{ax_o \equiv b \pmod{n}} \Leftrightarrow ax_o - b = ny, \text{ para algum } y \in \boldsymbol{Z}.$$

Desse modo, o problema de encontrar todas as soluções de uma congruência linear é idêntico ao de obter todas as soluções da equação diofantina $ax_o - ny = b$.

Na prática, tratamos como iguais duas soluções quaisquer da congruência $\boldsymbol{ax \equiv b \pmod{n}}$ *que não são côngruas módulo n,* mesmo que elas não sejam iguais no sentido tradicional. Por exemplo, x = 2 e x = 7 satisfazem a congruência linear $4x \equiv 3 \pmod{5}$. Como $2 \equiv 7 \pmod{5}$, tratamos 2 e 7 como a mesma solução da congruência linear $4x \equiv 3 \pmod{5}$. Ou seja, quando falamos do número de soluções da congruência linear $\boldsymbol{ax_o \equiv b \pmod{n}}$, estaremos contando somente aquelas que são *incongruentes módulo n.*

Uma questão: quando a congruência linear $\mathbf{ax_o \equiv b \pmod{n}}$ admite solução? E,nesse caso, quantas são as soluções incongruentes módulo n?
A resposta é dada pelo teorema seguinte.

Teorema 1
A congruência linear $\boldsymbol{ax_o \equiv b \pmod{n}}$ admite solução se, e somente se, d divide b, onde d = MDC(a, n). Além disso, se d divide b, então, a congruência admite d soluções mutuamente incongruentes módulo n.
Demonstração

Observe que a congruência linear dada é equivalente à equação diofantina $ax - ny = b$. Foi visto na aula 5 que a equação diofantina admite solução se, e somente se, $d = MDC(a, n)$ divide b. Além disso, as soluções da equação diofantina são da forma $x = x_o + \frac{n}{d}t$ e $y = y_o + \frac{a}{d}t$, com t um número inteiro.

Agora, dentre os inteiros x satisfazendo $x = x_o + \frac{n}{d}t$, considere aqueles para os quais t toma os valores seguintes $t = 1, 2, 3, ..., d - 1$. Ou seja, considere os d inteiros:

$$x_o,\ x_o + \frac{n}{d},\ x_o + \frac{2n}{d},\ x_o + \frac{3n}{d},\ x_o + \frac{4n}{d},\ldots,\ x_o + \frac{(d-1)n}{n}.$$

Para concluirmos a prova, vamos mostrar que esses inteiros são dois a dois incongruentes módulo n e qualquer inteiro x, que é solução da congruência dada, é congruente a algum dos inteiros acima.

De fato, se $x_o + \frac{n}{d}i \equiv x_o + \frac{n}{d}j \pmod{n}$, com $i, j \in \{0, 1, 2, ..., d-1\}$, com $i \geq j$. Assim, podemos escrever $\frac{n}{d}i \equiv \frac{n}{d}j \pmod{n}$. Agora, observe que $MDC(\frac{n}{d}, n) = \frac{n}{d}$ e, portanto, $\frac{n}{d}$ pode ser cancelado na última congruência obtida. Ou seja, depois do cancelamento, teremos $i \equiv j (mod\ d)$. Isso é o mesmo que dizer que d divide $(i - j)$. Mas, isso é impossível, pois $0 < i - j < d$.

Para concluir, resta mostrar que qualquer outra solução da congruência linear, $x = x_o + \frac{n}{d}t$, é congruente a algum dos d inteiros listados acima. Para isso, utilizamos o Algoritmo da Divisão, dividindo t por d: $t = qd + r$, onde $0 \leq r < d$. Assim, podemos escrever: $x = x_o + \frac{n}{d}t = x_o + \frac{n}{d}(qd + r) = x_o + nd + \frac{n}{d}r \equiv x_o + \frac{n}{d}r \pmod{n}$, onde $x = x_o + \frac{n}{d}r$ sendo um dos d números acima. O que conclui a prova.

Exemplo 16

Encontre todas as soluções da congruência linear $6x \equiv 21 \pmod{51}$.

Solução

As soluções da congruência linear $6x \equiv 21 \pmod{51}$ podem ser obtidas através da equação diofantina $6x - 51y = 21$, que admite solução, pois MDC(6, 51) = 3 divide 21. O teorema anterior garante a existência de 3 soluções incongruentes módulo 21. Por outro lado, uma solução da equação diofantina seria $x_o = -56$ e $y_o = -7$. Ou seja, as soluções da congruência linear $6x \equiv 21 \pmod{51}$ são:

$$x = -56 + \frac{51}{3}t \equiv 46 + 17t \pmod{51}, \text{ com t} = 0, 1, 2.$$

Assim, as soluções são: $x \equiv 46 \pmod{51}$, $x \equiv 12 \pmod{51}$ e $x \equiv 29 \pmod{51}$.

Exercício 9
Encontre todas as soluções da congruência linear $3x \equiv 1 \pmod 5$.

Exercícios

1) Resolva as seguintes congruências lineares
(a) $10x \equiv 5 \pmod{12}$ (b) $131x \equiv 21 \pmod{77}$

2) Qual é o resto da divisão de 19^{385} por 31?

3) Encontre o resto da divisão de:
(a) $1^5 + 2^5 + 3^5 + ... + 100^5$ por 4. (b) $1! + 2! + 3! + ... + 100!$ por 15.

4) Encontre todos os inteiros n tal que: $100 \leq n \leq 200$, e $3n \equiv 7 \pmod{19}$.

5) Ache um sistema completo de restos módulo 11 composto de múltiplos de 7.

Resumo
Nesta aula, estudamos a noção de congruência, introduzida por Gauss para inovar o estudo da Aritmética.

Referências

BURTON, David M. **Elementary number theory**. New York: McGraw-Hill, 1998.

COUTINHO, S. C. **Números inteiros e criptografia RSA**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada – IMPA/ Sociedade Brasileira de Matemática – SBM, 1997.

DU SAUTOY, Marcus. **A música dos números primos**: a história de um problema não resolvido. Rio de Janeiro: Jorge Zahar, 2008.

HEFEZ, Abramo. **Elementos de aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2005.

AULA 08 – O Teorema Chinês de Restos e o Pequeno Teorema de Fermat

Apresentação

Nesta aula, estudaremos a solução de sistemas de congruências lineares, baseado no que ficou conhecido como Teorema Chinês de Restos. Também estudaremos as idéias revolucionárias de Fermat, usadas hoje em dia para permitir o comércio eletrônico confiável.

Tente entender tudo que está sendo explicado na aula. Estude com caneta e papel ao lado. Leia com atenção. Se for preciso, leia várias vezes uma linha ou um parágrafo. Seja paciente e procure ter certeza que você entendeu o que (e por que) está fazendo.

Objetivos

Com esta aula espera-se que você possa:

- Resolver sistemas de congruências lineares, sob as condições do Teorema Chinês de restos*;*
- Aplicar corretamente o Teorema de Fermat;

O TEOREMA CHINÊS DE RESTOS

Problemas antigos da astronomia, ligados aos movimentos periódicos dos corpos celestes, deram origem ao hoje conhecido como Teorema Chinês de Restos. O nome veio do fato dos problemas terem sido originários dos antigos matemáticos chineses. Há registros de problemas relacionados ao tema propostos no século terceiro depois de Cristo.

Teorema 2 (O Teorema Chinês de Restos)
Sejam $n_1, n_2, n_3, \ldots, n_k$ números inteiros positivos tais que MDC$(n_i, n_j) = 1$, para $i \neq j$. O sistema de congruências lineares

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ x &\equiv a_3 \pmod{n_3} \\ &\ldots\ldots\ldots\ldots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

admite uma solução simultânea, que é única módulo o inteiro $n = n_1 n_2 n_3 \ldots n_k$.

Demonstração

Seja $n = n_1n_2n_3...n_k$. Para cada $r = 1, 2, 3, ..., k$, seja $N_r = \frac{n}{n_r} = n_1n_2n_3..n_{r-1}.n_{r+1}...n_k$. Isto é, N_r é o produto de todos os n_i, exceto o n_r. Como $MDC(n_i, n_j) = 1$, a congruência

$$N_r x \equiv 1 \pmod{n_r}$$

admite uma única solução, que chamaremos de x_r, pois $MDC(N_r, n_r) = 1$, e divide 1. A solução do sistema será:

$$\bar{x} = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 + ... + a_kN_kx_k$$

De fato, basta observar que:

(i) $N_i \equiv 0 \pmod{n_r}$, para $i \neq r$, pois n_r divide N_i

(ii) $\bar{x} = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 + ... + a_kN_kx_k \equiv a_rN_rx_r \pmod{n_r}$

(iii) Como escolhemos x_r satisfazendo $N_rx \equiv 1 \pmod{n_r}$, temos, necessariamente, $\bar{x} \equiv a_r.1 \equiv a_r \pmod{n_r}$

Resta-nos mostrar que a solução é única módulo $n = n_1n_2n_3...n_k$. Suponha que exista outra solução x'. Isto é, $\bar{x} \equiv a_r \pmod{n_r} \equiv x'$, para $r = 1, 2, 3, ..., k$. Assim, n_r divide $\bar{x} - x'$, para cada valor de r. Como $MDC(n_i, n_j) = 1$, temos, obrigatoriamente, que $n = n_1n_2n_3...n_k$ divide $\bar{x} - x'$. Portanto, $\bar{x} \equiv x' \pmod{n}$, o que conclui a prova do Teorema Chinês de Restos.

EXEMPLO 16

Use o Teorema Chinês de Restos para resolver o seguinte sistema de congruências lineares:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

Solução

Na notação do Teorema Chinês de Restos, temos:

$a_1 = 2, a_2 = 3, a_3 = 2;$
$n_1 = 3, n_2 = 5, n_3 = 7;$
$n = 3 . 5. 7 = 105;$
$N_1 = 5 . 7 = 35,\ N_2 = 3 . 7 = 21,\ N_3 = 3 . 5 = 15.$

As congruências $N_1x_1 \equiv 1 \pmod 3$, $N_2x_2 \equiv 1 \pmod 5$ e $N_3x_3 \equiv 1 \pmod 7$, são:

$35x_1 \equiv 1 \pmod 3$, que é o mesmo que $2x_1 \equiv 1 \pmod 3$, cuja solução é $x_1 \equiv 2 \pmod 3$;
$21x_2 \equiv 1 \pmod 5$, que é o mesmo que $x_2 \equiv 1 \pmod 5$;
$15x_3 \equiv 1 \pmod 7$, que é o mesmo que $x_3 \equiv 1 \pmod 7$.

Portanto, a solução do sistema é dada por

$\bar{x} = 2.35.2 + 3.21.1 + 2.15.1 \equiv 233 \pmod{105} \equiv 23 \pmod{105}$.

ATIVIDADE 10
Use o Teorema Chinês de Restos para resolver o seguinte sistema de congruências lineares:

$x \equiv 1 \pmod{12}$
$x \equiv 1 \pmod{5}$
$x \equiv 0 \pmod{7}$

EXEMPLO 17 (Antigo problema Chinês)
Uma senhora transportava um cesto de ovos. Assustada por um cavalo que galopava perto dela deixa cair o cesto e todos os ovos se partem. Quando lhe perguntaram quantos ovos tivera o cesto, respondeu dizendo que é muito fraca em aritmética, mas lembra-se de ter contado os ovos de dois em dois, de três em três, de quatro em quatro e de cinco em cinco, e tivera sobra de 1, 2, 3, e 4 ovos, respectivamente.

Ache a menor quantidade de ovos que o cesto inicialmente poderia ter.
Solução

Seja x a quantidade de ovos que estavam inicialmente no cesto. Podemos escrever:

$x \equiv 1 \pmod{2}$
$x \equiv 2 \pmod{3}$
$x \equiv 3 \pmod{4}$
$x \equiv 4 \pmod{5}$

Na notação do Teorema Chinês de Restos, temos:

$a_1 = 1, a_2 = 2, a_3 = 3, a_4 = 4;$
$n_1 = 2, n_2 = 3, n_3 = 4, n_4 = 5;$

Não podemos aplicar diretamente o Teorema Chinês de Restos, pois $MDC(n_1, n_2) = MDC(2, 4) = 1$. Para resolver o problema, inicialmente, trabalhamos somente com as congruências lineares

$x \equiv 1 \pmod{2}$
$x \equiv 2 \pmod{3}$
$x \equiv 4 \pmod{5}$

Agora, na notação do Teorema Chinês de Restos o sistema acima tem os seguintes dados:

$a_1 = 1, a_2 = 2, a_3 = 4;$
$n_1 = 2, n_2 = 3, n_3 = 5;$
$n = 2 . 3. 5 = 30,$
$N_1 = 3 . 5 = 15, \ N_2 = 2 . 5 = 10, \ N_3 = 2 . 3 = 6.$

As congruências $N_1x_1 \equiv 1 \pmod{2}$, $N_2x_2 \equiv 1 \pmod{3}$ e $N_3x_3 \equiv 1 \pmod{5}$, são:

$15x_1 \equiv 1 \pmod{2}$, que é o mesmo que $1x_1 \equiv 1 \pmod{2}$, cuja solução é $x_1 \equiv 1 \pmod{12}$,
$10x_2 \equiv 1 \pmod{3}$, que é o mesmo que $x_2 \equiv 1 \pmod{3}$, cuja solução é $x_2 \equiv 1 \pmod{3}$
$6x_3 \equiv 1 \pmod{5}$, que é o mesmo que $x_3 \equiv 1 \pmod{5}$, cuja solução é $x_3 \equiv 1 \pmod{7}$

Portanto a solução do sistema é dada por

$$\bar{x} = 1.15.1 + 2.10.1 + 4.6.1 \equiv 59 \pmod{30} \equiv 29 \pmod{30}$$

Ou seja, $\bar{x} = 29 + 30k$, onde k é um número inteiro. Agora, substituímos $\bar{x}$ na congruência $x \equiv 3 \pmod 4$.
Assim, $29 + 30\,k \equiv 3 \pmod 4$, que é o mesmo que $1 + 2k \equiv 3 \pmod 4$. Ou ainda:
$3 + 1 + 2k \equiv 3 + 3 \pmod 4$, que nos leva para $2k \equiv 2 \pmod 4$, que é equivalente a dizer $2k - 2 = 4t$, onde t é um inteiro. Ou seja, $2(k - 1) = 4t$. Portanto, k tem de ser um número ímpar, $k = 2s + 1$, onde s é um número inteiro. Portanto, $\bar{x} = 29 + 30(2s + 1) = 59 + 60s$,
Deste modo, o número mínimo de ovos que a cesta inicialmente poderia conter é 59.

O PEQUENO TEOREMA DE FERMAT

O mais famoso teorema de Fermat é conhecido como o Último Teorema de Fermat:

(**Último Teorema de Fermat)** Se n é um inteiro maior do que 2, a equação $x^n + y^n = z^n$ não admite solução x, y e z no conjunto dos números inteiros maiores do que 1.

Pierre de Fermat (1601-1665) foi um matemático e cientista francês. Seu pai, Dominique de Fermat, era um rico mercador de peles e lhe propiciou uma educação privilegiada, inicialmente no mosteiro franciscano de Grandselve e depois na Universidade de Toulouse. Ingressou no serviço público em 1631. Em 1652 ele foi promovido para Juiz Supremo na Corte Criminal Soberana do Parlamento de Toulouse, todavia esta promoção se deu em ocorrência da chegada da praga, que levou a vida de grande parte da população da Europa. Neste mesmo ano Fermat também adoeceu e chegou-se a afirmar que ele havia morrido, entretanto ele se recuperou e permaneceu vivo por mais de uma década. Sua morte, de fato, deu-se a 12 de Janeiro de 1665, em Castres.

Em razão de seu cargo, Fermat não podia ter muitos amigos para não ser acusado de favoritismo em seus julgamentos, também em razão da tumultuada fase que passava a França de então, com o Cardeal Richelieu sendo primeiro-ministro. Ao se investigar a produção matemática de Fermat, percebe-se facilmente a característica amadora predominante em seus trabalhos. Na verdade, com pouquíssimas exceções, ele não publicou nada em vida e nem fez qualquer exposição sistemática de suas descobertas e de seus métodos, tinha as questões da matemática mais como desafios a serem resolvidos.

Considerado o Príncipe dos amadores, Pierre de Fermat nunca teve formalmente a matemática como a principal atividade de sua vida. Jurista e magistrado por profissão, dedicava à Matemática apenas suas horas de lazer e, mesmo assim, foi considerado por Pascal o maior matemático de seu tempo.

Contudo, seu grande gênio matemático perpassou várias gerações, fazendo com que várias mentes se debruçassem com respeito sob o seu legado, que era composto por

contribuições nas mais diversas áreas das matemáticas, as principais: cálculo geométrico e infinitesimal; teoria dos números; e teoria da probabilidade. Entre os estudiosos com os quais mantinha contato postal, estão: Sir Kenelm Digby, John Wallis, Nicholas Hensius, além de Blaise Pascal, Assendi, Roberval, Beaugrand e o padre Marin Mersenne.

O interesse desperto em Fermat pela Matemática, possivelmente, deu-se com a leitura de uma tradução latina, feita por Claude Gaspar Bachet de Méziriac, de Aritmética de Diophante, um texto sobrevivente da famosa Biblioteca de Alexandria, queimada pelos árabes no ano 646 d.C., e que compilava cerca de dois mil anos de conhecimentos matemáticos.

A matemática do século XVII estava ainda se recuperando da Idade das Trevas, portanto não é de se admirar o caráter amador dos trabalhos de Fermat. No entanto, se ele era um amador, então era o melhor deles, devido à precisão e à importância de seus estudos, que, diga-se ainda, estavam sendo realizados longe de Paris, o único centro que abrigava grandes matemáticos, mas até então ainda não prestigiados estudiosos da Matemática, como Pascal, Gassendi, Mersenne, entre outros.

O padre Marin Mersenne teve um papel importante na história da matemática francesa do século XVII e também foi uma das poucas amizades de Fermat. Todavia, é interessante observar mais de perto o desenvolvimento da Matemática nesta época.

Diferentemente da famosa escola pitagórica, os franceses não tinham o costume de trocar com os colegas os avanços recentes de suas pesquisas, devido à influência dos cosistas do século XVI, italianos que utilizavam símbolos para representar quantidades desconhecidas. Mersenne tinha o costume, desagradável para seus contemporâneos matemáticos, de divulgar os trabalhos dos pesquisadores. Em suas viagens pela França e por países estrangeiros, acabou conhecendo Fermat e trocando com ele várias correspondências. No entanto, mesmo com a insistência do padre, Fermat não publicou nada. (Fonte:http://pt.wikipedia.org/wiki/Pierre_de_Fermat)

Contam os historiadores que, em 1637, Fermat afirmou que tinha uma prova para a proposição que ficou conhecida com o Último Teorema de Fermat. Ele escreveu sua afirmação nas margens do livro de Diofanto, *Arithmeticae,* uma versão feita por Claude Gaspar Bachet (1581–1683). Ele afirmou: "*Tenho uma prova maravilhosa para esta proposição, mas a margem é muito pequena para cabê-la*". Muitos matemáticos tentaram, sem sucesso, uma prova: Euler, Gauss, Dirichlet, Legendre, Lamé, Kummer, Dedekind etc.

Em setembro de 1994, o matemático Andrew Wiles, de Princeton, e seu estudante Richard Taylor concluíram uma prova usando fatos sobre curvas elípticas, que está muito acima do nível desta aula. Portanto, nesta aula não trataremos do Último Teorema de Fermat. Estudaremos, em vez dele, o Pequeno Teorema de Fermat.

Numa carta para Bernard Frenicle de Bessy (1605–1675), datada de 18 de outubro de 1640, Pierre de Fermat (1601 – 1665) deu sua versão do que hoje conhecemos como Pequeno Teorema de Fermat. Ele descobriu algo surpreendente e que foi usado para a criação do sistema RSA, já comentado na Aula 05.

Fermat descobriu que se você, por exemplo, calcular as potências de 2 em uma calculadora comum e verificar o resto na divisão por 7, estes restos têm um padrão: começando com 2^0, após 6 cálculos consecutivos o resto volta e ser 1, veja a tabela a seguir:

Tabela 1 – As potências de 2 e seus restos na divisão por 7.

Potência de 2	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}
Visor da Calculadora	1	2	4	8	16	32	64	128	256	512	1024	2048	4096
Resto da Divisão por 7	1	2	4	1	2	4	1	2	3	1	2	4	1

Fermat, ainda viu que este padrão se mantinha se ele substituísse 7 por qualquer número primo, enunciando o seguinte:

Teorema 3 (Pequeno Teorema de Fermat)
Se p é um número primo e a é um inteiro que não é divisível por p, então

$$a^{p-1} \equiv 1 \pmod{p}$$

Demonstração

Consideremos os primeiros p – 1 múltiplos inteiros positivos de *a*:

a, 2a, 3a, 4a, ..., (p -2)a, (p – 1)a.

Inicialmente, vamos provar que nenhum desses múltiplos de *a* é côngruo a qualquer outro módulo *p*, nem é congruente a zero módulo *p*. Para isso, vamos supor que existam números inteiros *r* e *s*, com $1 \le r < s \le p - 1$ satisfazendo

$$ra \equiv as \pmod{p}.$$

Como MDC(*p, a*) = 1, podemos cancelar *a* na congruência acima e obter

$$r \equiv s \pmod{p},$$

com $1 \le r < s \le p - 1$, que é uma contradição. Como os restos possíveis na divisão por *p* são 1, 2, 3, ..., *p* – 1, os números *a, 2a, 3a, 4a, ..., (p -2)a, (p – 1)a* tem de ser congruentes, em alguma ordem, a: 1, 2, 3, ..., *p* – 1. Agora, multipliquemos essas congruências membro a membro para obter

$$a.\ 2a\ .3a.\ 4,\ \ldots\ (p-2)a.\ (p-1)a \equiv 1.\ 2.\ 3\ \ldots\ (p-2).(p-1) \pmod{p}$$

Que é o mesmo que escrever:

$$a^{p-1}.\ 1.\ 2.\ 3\ \ldots\ (p-2).(p-1) \equiv 1.\ 2.\ 3\ \ldots\ (p-2).(p-1) \pmod{p}$$

Ou seja, $a^{p-1}.(p-1)! \equiv (p-1)! \pmod{p}$.

Agora, observe que p não divide $(p-1)!$, pois no desenvolvimento de $(p-1)!$ o número p não comparece. Portanto, na última congruência, podemos cancelar $(p-1)!$, obtendo $a^{p-1} \equiv 1 \pmod{p}$, como queríamos.

EXEMPLO 18
Use o Pequeno Teorema de Fermat para verificar que 17 divide $11^{104} + 1$.
Solução

17 é um número primo e 11 não divide 17. Assim, pelo Pequeno Teorema de Fermat, $11^{16} \equiv 1 \pmod{17}$. Por outro lado, pelo Algoritmo da Divisão, $104 = 16 \cdot 6 + 8$.
Assim, $11^{104} = (11^{16})^6.11^8 \equiv (1)^6.11^8 \pmod{17} \equiv 11^8 \pmod{17}$. Agora, observe que:
$11^2 = 121 \equiv 2 \pmod{17}$ e $11^8 = (11^2)^4 \equiv 2^4 \pmod{17} \equiv -1 \pmod{17}$. Portanto, podemos afirmar que $11^{104} \equiv 11^8 \pmod{17} \equiv -1 \pmod{17}$, que é o mesmo que afirmar que 17 divide $11^{104} + 1$.

ATIVIDADE 11
Usando o Pequeno Teorema de Fermat, provar que 18^{12} deixa resto 1 quando dividido por 7.

EXEMPLO 19
Encontre o resto da divisão de 3^{600} por 7.
Solução

Pelo Pequeno Teorema de Fermat, podemos escrever $3^6 \equiv 1 \pmod{7}$. Assim,
$3^{600} = (3^6)^{100} \equiv (1)^{100} \pmod{7} \equiv 1 \pmod{7}$. Portanto, o resto da divisão de 3^{600} por 7 é 1.
ATIVIDADE 12
Ache o menor inteiro positivo n para o qual o número $2^{n-1} - 1$ é divisível por 41.

EXEMPLO 20
Existe um inteiro positivo c menor do que 40, para o qual 41 divide $2^c - 1$?
Solução

Vamos supor que exista. Pelo Princípio da Boa Ordem ou Princípio da Boa Ordenação, existe o menor desses números. Chamemos d o menor inteiro positivo para o qual 41 divide $2^d - 1$. Isto é, $2^d = 1 + 41t$, onde t é um número inteiro. Pelo Algoritmo da Divisão, $40 = qd + r$, com $0 \leq r < d$. Agora, podemos escrever $2^{qd} = (1 + 41t)^q$ e, aplicando o Binômio de Newton, podemos desenvolver $(1 + 41t)^q$ e verificar que $2^{qd} = (1 + 41t)^q = 41m + 1$, onde m é um número inteiro. Mas, como $2^{40} = 2^{qd + r} = 1 + 41k$, temos $1 + 41k = 2^{qd} .2^r = (1 + 41m).\ 2^r$. Usando o Algoritmo da Divisão, $2^r = 41v + s$, com $0 \leq s < 41$. Daí segue que

$$1 + 41k = 2^{qd} .2^r = (1 + 41m).\ (41v + s) = 41b + s,$$ o que implica $s = 1$. Portanto,

$2^r = 41v + s = 41v + 1$ e $2^r - 1$ é divisível por 41. Mas, $0 \leq r < d$ e d é o menor inteiro positivo com esta propriedade. Contradição. Portanto, $r = 0$ e d divide 40. Então o número inteiro d tem de pertencer ao conjunto $\{1, 2, 4, 5, 8, 10, 20, 40\}$. Verificando esses valores, temos

$2^1 - 1 = 1$, que não é divisível por 41; $2^2 - 1 = 3$, que não é divisível por 41;
$2^4 - 1 = 15$, que não é divisível por 41; $2^5 - 1 = 31$, que não é divisível por 41;
$2^8 - 1 = 255$, que não é divisível por 41; $2^{10} - 1 = 1023$, que não é divisível por 41;
$2^{20} - 1 = 1048575 = 41 \times 25575$, que é, portanto, divisível por 41;
$2^{40} \equiv 1 \pmod{41}$.

Deste modo, 20 é o menor número tal que $2^{20} - 1$ é divisível por 41.

O Pequeno Teorema de Fermat nos garante que: se $p = 41$, então $2^{40} - 1$ é divisível por 41. O Exemplo 20 nos mostra que é possível que algum divisor d de $p - 1$ tenha também esta propriedade: $2^d - 1$ é divisível por 41.

O Pequeno Teorema de Fermat pode ser enunciado de uma forma mais compacta, eliminando-se a condição de que o número primo p não divide a:

Corolário 1
Se p é um número primo, então $a^p \equiv a \pmod{p}$, para todo número inteiro a.
Demonstração

De fato, se p divide a, então $a^p \equiv 0 \pmod{p} \equiv a \pmod{p}$. Agora, se p não divide a, segue, pelo Pequeno Teorema de Fermat, que $a^{p-1} \equiv 1 \pmod{p}$. Multiplicando cada membro da congruência por a, obtemos $a^p \equiv a \pmod{p}$.

EXEMPLO 21
Encontre o resto da divisão de 3^{102} por 101.
Solução

Pelo Corolário do Pequeno Teorema de Fermat, temos $3^{101} \equiv 3 \pmod{101}$. Por outro lado, $3^{102} = 3^{101}.3 \equiv 3 \,.\, 3 \equiv \pmod{101}$. Portanto, o resto da divisão de 3^{102} por 101 é 9.

ATIVIDADE 13
Encontre o resto da divisão de 8^{900} por 29.

O TEOREMA DE WILSON
Em 1770, Eduard Waring (1734–1798), matemático inglês, afirmou em seu livro *Medidationes algebraicae,* que um de seus estudantes, John Wilson (1741 – 1793), conjecturou que, se p é um número inteiro primo, então p divide $(p - 1)! + 1$. Mas, Wilson não conseguiu provar. O resultado foi provado por Legendre, em 1771, que provou também a recíproca.

Teorema 4 (Wilson)
Se p é um número primo, então $(p-1)! \equiv -1 \pmod{p}$
Demonstração

Se $p = 2$, teremos $(2 - 1)! = 1 \equiv -1 \pmod{2}$.
Se $p = 3$, teremos $(3 - 1)! = 2! = 2 \equiv -1 \pmod{3}$.

Assim, nos casos em que $p = 2$ ou $p = 3$ a afirmação é óbvia. Suponha que p seja um primo qualquer maior do que 3. Suponha que $a \in \{1, 2, 3, ..., p - 2, p-1\}$.
Considere a congruência linear

$$ax \equiv 1 \ (mod \ p).$$

Como MDC(a, p) = 1, a congruência admite uma única solução módulo p. Assim, existe um único inteiro b, com $1 \leq b \leq p - 1$, satisfazendo

$$ab \equiv 1 \pmod{p} \quad (*)$$

Ou seja, existe o inverso de a módulo p. Como p é primo, temos que $a = b$, se e somente se, $a = 1$ ou $a = p - 1$. Para verificarmos este fato, basta observar que: $a^2 \equiv 1 \pmod{p} \Leftrightarrow a^2 - 1 \equiv 0 \pmod{p} \Leftrightarrow (a - 1).(a + 1) \equiv 0 \pmod{p}$. Portanto, ou $a - 1 \equiv 0 \pmod{p}$ ou $a + 1 \equiv 0 \pmod{p}$, que é equivalente a dizer: ou a 1(mod p) ou a $p - 1 \pmod{p}$. Para cada a pertencente ao subconjunto {2, 3, 4, ..., (p – 2)}, existe b, seu inverso módulo p, com a distinto de b. Deste modo, existem $\frac{p-3}{2}$ congruência do tipo (*). Multiplicando membro a membro todas elas, obtemos:

$$2.3.4....(p - 3).(p-2) \equiv 1 \pmod{p}$$

Ou ainda, $(p - 2)! \equiv 1 \pmod{p}$. Agora, multiplicando $(p - 1)$ de cada lado, obtemos:

$(p - 1).(p - 2)! \equiv (p - 1).1 \pmod{p} \equiv -1 \pmod{p}$, como queríamos.

EXERCÍCIOS

1) Um bando de 19 piratas roubam uma sacola com moedas de ouro. Quando eles tentaram dividir a fortuna em partes iguais, sobraram 3 moedas. Na discussão sobre quem ficava com as três moedas que sobraram, um pirata foi morto. A seguir, na divisão das moedas em partes iguais entre os sobreviventes, sobraram 10 moedas. Novamente, surgiu uma disputa pela posse das dez moedas que sobraram e um pirata foi morto. Agora, o total das moedas foi distribuído, igualmente, entre os sobreviventes sem sobrar qualquer moeda.

Qual é o menor número de moedas que a sacola poderia conter?

(Sugestão: Use o teorema Chinês de Restos))

2) Mostre que:

(a) 7 divide $1941^{1963} + 1963^{1991}$. (b) 39 divide $53^{103} + 103^{53}$.

3) Qual é o resto da divisão de 19^{385} por 31?

4) Mostre que:

(a) 7 divide $1941^{1963} + 1963^{1991}$. (b) 39 divide $53^{103} + 103^{53}$.

5) Três fazendeiros cultivavam junto todo o seu arroz e o dividiam igualmente entre si no tempo da colheita. Certo ano, cada um deles foi a um mercado diferente vender seu arroz. Cada um destes mercados só comprava arroz em múltiplos de um peso padrão, que diferia em cada um dos mercados. O primeiro fazendeiro vendeu o seu arroz em um mercado onde o peso padrão era 87 kg. Ele vendeu tudo o que podia e voltou para casa com 18 kg. O segundo fazendeiro vendeu todo o arroz que podia ser vendido em um mercado cujo peso padrão era 170 kg e voltou para casa com 58 kg. O terceiro fazendeiro vendeu todo o arroz que podia em um mercado cujo peso era de 143 kg e voltou (ao mesmo tempo em que os outros dois) com 40 kg. Qual a quantidade mínima de arroz que eles podiam ter cultivado, no total?

(Sugestão: Use o Teorema Chinês de Restos)

6) Encontre o menor inteiro a maior do que 2 tal que 2 divide a, 3 divide $a+1$, 4 divide $a+2$, 5 divide $a+3$ e 6 divide $a+4$.

7) Numa ilha tropical, 5 homens e um macaco passam o dia todo recolhendo coco. À noite, quando todos dormem, um dos homens levanta-se e, sem avisar aos outros, resolve tomar sua parte. Para isso, divide os cocos em cinco pilhas iguais, restando um coco, que ele dá ao macaco. Depois de esconder a sua parte, colocar os cocos restantes numa só pilha, vai dormir. Cada um dos homens levanta-se, sem avisar aos outros, e procede da mesma maneira, sendo que, toda vez que fazem a divisão da pilha em cinco partes iguais, sobra um coco, que é dado ao macaco. Na manhã seguinte, todos os homens levantam-se e dividem os cocos que restaram em cinco partes iguais, tendo sobrado, também, um coco, que é dado ao macaco.
Ache o número mínimo de cocos que poderia ter na pilha original.

(Sugestão: Seja n a quantidade de cocos que cada homem recebeu na divisão da manhã seguinte, onde a pilha era formada por $5n + 1$ cocos. O quinto homem que acessou a pilha na noite anterior pegou $\frac{5n+1}{4}$ cocos. Quantos cocos existia na pilha quando o quinto homem interveio?)

8) O mágico senta-se numa cadeira, de costas voltadas para a audiência. Alguém pensa num número natural qualquer não superior a 105. Divide o número por 3 e diz o resto da divisão ao mágico. Em seguida, divide o número inicialmente pensado por 5 e fala o resto da divisão ao mágico. E, finalmente, divide o número pensado por 7 e diz o resto. O mágico, conhecendo apenas os três restos, advinha o número pensado.
Qual é o truque?

(Sugestão: Observe que MDC(3, 5, 7) = 1. Use o Teorema Chinês de Restos)

9) Mostre que 39 divide o número $53^{103} + 103^{53}$.

RESUMO

Nesta aula, estudamos a solução de sistemas de congruências lineares e vimos também às idéias de Fermat, que são usadas hoje em dia, para tornar o comércio eletrônico confiável.

REFERÊNCIAS

Burton, David M. – **Elementary Number Theory**. The McGraw-Hill Companies, Inc. New York. USA. 1998

Coutinho, S. C. – **Números Inteiros e Criptografia RSA**. Instituto de Matemática Pura e Aplicada – IMPA & Sociedade Brasileira de Matemática – SBM. Rio de Janeiro. 1997

Du Sautoy, Marcus – **A Música dos Números Primos: A História de um Problema não Resolvido**. Zahar. Rio de Janeiro. 2008

Hefez, Abramo – **Elementos de Aritmética**. Sociedade Brasileira Matemática. Rio de Janeiro. 2005

AULA 09 – A Função de Euler

Apresentação

Nesta aula, estaremos interessados em determinar a quantidade de números naturais relativamente primos com um número natural n e menores do que n. Em seguida, veremos como usar este fato para generalizar o Pequeno Teorema de Fermat, estudado na Aula 08.

Tente entender tudo que está sendo explicado na aula. Estude com caneta e papel ao lado. Leia com atenção. Se for preciso, leia várias vezes uma linha ou um parágrafo. Seja paciente e procure ter certeza que você entendeu o que (e por que) está fazendo.

Objetivos

Espera-se que ao término desta aula você seja capaz de:

1 Saber calcular os valores da função de Euler em um número inteiro positivo, conhecida sua decomposição em fatores primos*;*

2 Usar o Teorema de Euler em problemas do tipo: encontrar o resto da divisão de um número inteiro quando dividido por outro.

1. A FUNÇÃO DE EULER

Dado um número natural n é importante saber a quantidade de números naturais menores do que n e relativamente primos com n. Essa curiosidade nos remete à definição da chamada *função de Euler:*

$\varphi : \mathbf{N} \rightarrow \mathbf{N}$, tal que $n \in \mathbf{N}$
$\varphi(n)$ = a quantidade de números naturais $k < n$, tais que k e n são primos entre si.

Vejamos os seguintes exemplos de $\varphi(n)$ para alguns valores particulares de n.

EXEMPLO 1
$\varphi(1) = 1$, $\varphi(2) = 1$ e $\varphi(n) \geq 2$, para todo número natural $n \geq 3$.
Solução

O único número $k \leq 1$ relativamente primo com 1 é o próprio 1. Logo, $\varphi(1) = 1$. O mesmo vale para 2. Ou seja, o único número relativamente primo com 2 e menor do que 2 é o 1. Isso nos diz que $\varphi(2) = 1$.
Agora, para $n \geq 3$, temos que $n - 1 \geq 2$. Como dois números consecutivos são sempre primos entre si, segue que, para $n \geq 3$, n e $n - 1$ são relativamente primos e o mesmo acontece com 1 e n, o que dá $\varphi(n) \geq 2$.

EXERCÍCIO 1
Encontre os valores:
(a) $\varphi(8)$ (b) $\varphi(11)$ (c) $\varphi(14)$

Agora podemos ver algumas proposições de caráter mais geral.

PROPOSIÇÃO 1
Dado um número natural n, então: $\varphi(n) = n - 1$ se, e somente se, n é um número primo.
Demonstração

Suponha que $\varphi(n) = n - 1$. Isso significa que todos os $n - 1$ números naturais menores do que n são relativamente primos com n. Logo, n não pode ser de composto num produto de fatores primos menores do que n. Ou seja, n é um número primo.
Reciprocamente, supondo n primo, então todos os números naturais menores do que n são relativamente primos com n. Mas, os números naturais menores do que n são precisamente 1, 2, 3, 4, ..., $n - 1$. Logo, $\varphi(n) = n - 1$.

Seguindo essa linha de raciocínio, a próxima pergunta é saber se existe também uma fórmula para calcular $\varphi(n)$, onde n é a potência de um número primo. Tal fórmula existe e é dada pelo seguinte:

PROPOSIÇÃO 2
Se $n = p^r$, onde p é um número primo e $r \geq 1$, então $\varphi(n) = p^{r-1}(p - 1)$.

Demonstração

Como p é um número primo, então todos os números inteiros positivos menores do que ou iguais a $n = p^r$ que não são relativamente primos com n são todos aqueles que têm alguma potência de p como fator, a saber: os p^{r-1} números 1.p, 2.p, 3.p, ..., $p^{r-1}.p = p^r$. Portanto, todos os outros números inteiros variando de 1 a p^r são relativamente primos com n, o que nos dá $\varphi(n) = p^r - p^{r-1}$. Isto é, $\varphi(n) = p^{r-1}(p - 1)$.

COROLÁRIO
Sejam *r, s* inteiros maiores do que ou iguais a 1 e p um número primo. Então
$\varphi(p^r).\ \varphi(p^s) < \varphi(p^{r+s})$.
Demonstração

Pela Proposição, temos:

$$\varphi(p^r).\ \varphi(p^s) = p^{r-1}(p - 1).\ p^{s-1}(p - 1) = p^{r+s-2}(p - 1)^2 =$$
$$= p^{r+s-1}.\left(\frac{p-1}{p}\right).(p-1)\,.$$

Ora, $\frac{p-1}{p} < 1$. Logo, $\varphi(p^r).\ \varphi(p^s) < p^{r+s-1}.(p - 1) = \varphi(p^{r+s})$.

EXEMPLO 2
Como 19 é um número primo, então $\varphi(19) = 19 - 1 = 18$.
Enquanto $\varphi(125) = \varphi(5^3) = 5^2.(5 - 1) = 25 \times 4 = 100$.
Do mesmo modo, $\varphi(81) = \varphi(3^4) = 3^3.(3 - 1) = 27 \times 2 = 54$.

EXERCÍCIO 2
Calcule a soma $1 + \varphi(11) + \varphi(11^2) + \varphi(11^3) + ... + \varphi(11^n)$.
Qual é a resposta se substituirmos 11 por um número primo *p* qualquer?

Continuando com o mesmo tipo de curiosidade de antes, poderíamos indagar:

É possível encontrar uma fórmula para φ(n) em função dos fatores primos da decomposição de n?

A resposta é sim, o que explicaremos a seguir. Mas, antes dessa explicação, há um caminho a percorrer que começa com o seguinte resultado:

LEMA 1
Dado um número natural $n > 1$, todo sistema completo de restos módulo n está em correspondência biunívoca com o conjunto $S_0 = \{0, 1, 2, ..., n - 1\}$.
Nota: Por isso $S_0 = \{0, 1, 2, ..., n - 1\}$ é dito um *sistema fundamental completo de restos módulo n*.
Demonstração

Na Aula 07 foi definido que um conjunto $S = \{x_1, x_2, ..., x_n\}$ de n números naturais é dito um *sistema completo de restos módulo n*, se dois quaisquer de seus elementos não são congruentes módulo n, isto é, x_i não é congruente a x_j módulo n, se $i \neq j$.
Pelo Algoritmo da Divisão, para cada j, com $1 \leq j \leq n$, existem inteiros q_j e r_j tais que:

$$x_j = q_j.n + r_j, \text{ onde } 0 \leq r_j \leq n.$$

Como $x_j - x_i = (q_j - q_i).n + (r_j - r_i)$, se fosse $r_j = r_i$, teríamos $x_j - x_i = (q_j - q_i).n$. Isto é, $x_j \equiv x_i \pmod{n}$, o que é contrário à hipótese. Logo, a função que a cada x_j associa o resto r_j da divisão de x_j por n, define uma correspondência biunívoca entre os conjuntos S e S_0, pois S possui n elementos e a cada elemento de S é associado a um único elemento de S_0 que possui também n elementos.

O próximo passo é estabelecer o seguinte:

TEOREMA 1
Se m e n são números inteiros positivos primos entre si, então $\varphi(m.n) = \varphi(m).\varphi(n)$.
Demonstração

Seja $0 \leq z < mn$ um inteiro. A divisão de z por n pode ser expressa como

$$z = nq + r, \text{ onde } 0 \leq r < n.$$

Sendo $0 \leq z < mn$, segue que $0 \leq q \leq m - 1$.
De fato, se fosse $q > m - 1$, teríamos $q \geq m$ e teríamos $z = nq + r \geq mn + r \geq mn$.
Ou seja, $z \geq mn$, o que é uma contradição.

O fato crucial para nossa prova é que, para cada $0 \leq r < n$, o conjunto com m elementos

$$S_r = \{r, n + r, 2n + r, 3n + r, ... , (m - 1).n + r\}$$

é um sistema completo de restos módulo m quando m e n são primos entre si, que é o nosso caso.
Para tanto, sejam $kn + r$ e $jn + r$ dois elementos de S_r. Se tivéssemos

$$kn + r \equiv jn + r \pmod{m}$$

a lei do cancelamento implicaria que $kn \equiv jn \pmod{m}$. Como m e n são primos entre si, então n pode ser cancelado e obteríamos $k \equiv j \pmod{m}$. Mas, k e j estão entre 0 e $m - 1$, logo $k = j$, o que nos dá $kn + r = jn + r$. A conclusão é que dois elementos distintos quaisquer de S_r não são congruentes módulo m. Como S_r possui m elementos, segue que o mesmo é um sistema completo de restos módulo m.
Na Aula 05 vimos que, se *b = q. a + r, com 0 ≤ r < a, então MDC(a, b) = MDC(a, r).*
Desse modo, se $0 \leq z < mn$ é um número relativamente primo com mn e como m e n são primos entre si, então z é também relativamente primo com m e com n. Como
$z = qm + r$, onde $0 \leq r < m$ e $z = kn + s$, onde $0 \leq s < n$, então z é relativamente primo com r e s, de acordo com o que vimos na Aula 05.
Observando isso, sejam:

A = {números naturais relativamente primos com mn e menores do que mn}
B = {números naturais relativamente primos com m e menores do que m}
C = {números naturais relativamente primos com n e menores do que n}.

Veja que A possui $\varphi(mn)$ elementos, B possui $\varphi(m)$ elementos e C tem $\varphi(n)$ elementos. Dado $z \in A$, então $z = qm + r$, onde $0 \leq r < m$. Como $z \in S_r$, existe $0 \leq s < n$ tal que

$z = kn + s$. Como $MDC(z, m) = 1$, segue que $MDC(r, m) = 1$. Logo, $r \in B$. Analogamente, concluímos que $s \in C$. Agora, definimos a função

$$f : A \rightarrow B \times C, \text{ pondo } f(z) = (r, s).$$

Mostraremos que f é uma bijeção.
Como o resto e o quociente obtidos pelo Algoritmo da Divisão são únicos, segue que f é uma função injetiva. Por outro lado, dado $(r, s) \in B \times C$, como S_r é um sistema completo de restos módulo m, escolha $z \in S_r$ tal que $z = kn + s$ e como z é um elemento de S_r, segue que $z = qm + r$.
Como $MDC(r, m) = 1$ e $MDC(s, n) = 1$, então $MDC(z, Mn) = 1$, pois m e n são primos entre si, isso nos diz que $z \in A$, $f(z) = (r, s)$ e logo f é sobrejetiva. Como A possui $\varphi(mn)$ elementos, B possui $\varphi(m)$ elementos e C tem $\varphi(n)$ elementos, então $B \times C$ possui $\varphi(m).\varphi(n)$ elementos. Portanto, $\varphi(m.n) = \varphi(m).\varphi(n)$.

COROLÁRIO 1
Se $m_1, m_2, m_3, ..., m_n$ são números inteiros positivos, dois a dois primos entre si, então

$$\varphi(m_1\, m_2\, m_3 ... \, m_n) = \varphi(m_1).\varphi(m_2).\varphi(m_3).....\varphi(m_n)$$

Demonstração

A demonstração será feita por indução sobre o número n de fatores.

- Para $n = 1$, o primeiro e o segundo membro da expressão são iguais a $\varphi(m_1)$.
- Suponha que a expressão válida para $n = k$. Isto é,

$$\varphi(m_1\, m_2\, m_3 ... \, m_k) = \varphi(m_1).\varphi(m_2).\varphi(m_3).....\varphi(m_k).$$

Mostraremos que ela é válida para $n = k + 1$.
Tomemos $m_1, m_2, m_3, ..., m_k, m_{k+1}$ são números inteiros positivos, dois a dois primos entre si. Isto é $MDC(m_i, m_j) = 1$, se $i \neq j$. Desse modo, chamando $a = m_1\, m_2\, m_3 ... \, m_k$, temos $MDC(a, m_{k+1}) = MDC(m_1\, m_2\, m_3 ... \, m_k\, m_{k+1}) = 1$, pois cada fator primo de m_j, para cada $1 \leq j \leq k$, é diferente de cada fator primo de m_{k+1}.
Como a e m_{k+1} são primos entre si, pelo Teorema 1,

$$\varphi(m_1\, m_2\, m_3 ... \, m_k\, m_{k+1}) = \varphi(am_{k+1}) = \varphi(a).\varphi(m_{k+1}) = \varphi(m_1\, m_2\, m_3 ... \, m_k).\varphi(m_{k+1}) =$$
$$= \varphi(m_1).\varphi(m_2).\varphi(m_3).....\varphi(m_k)\,).\varphi(m_{k+1}).$$

Isso garante que a fórmula proposta é válida para $n = k + 1$. Portanto, ela é válida para todo número natural n.

Uma propriedade interessante de φ é dada no seguinte:

COROLÁRIO 2

Para todo número inteiro $n > 2$, $\varphi(n)$ é par.
Demonstração

Se n contém um fator primo $p \geq 3$ na sua decomposição, seja p^r a maior potência de p nesta decomposição. Então podemos escrever $n = p^r.b$, onde p e b são primos entre si. Pelo Teorema 1, segue-se que $\varphi(n) = \varphi(p^r).\ \varphi(b) = p^{r-1}.(p - 1).\ \varphi(b)$. Como $p \geq 3$ é um número primo, em particular $p - 1$ é um número par. Logo, $\varphi(n)$ é par.
Por outro lado, se $n > 2$ não contém fator primo impar na sua decomposição em fatores primos, então $n = 2^k$, para $k > 1$, donde $\varphi(n) = \varphi(2^k) = 2^{k-1}.(2 - 1) = 2^{k-1}$. Como $k > 1$, segue que $\varphi(n)$ é par.

OBSERVAÇÃO 1
Para m e n primos entre si, o fato de $\varphi(m.n) = \varphi(m).\varphi(n)$, conforme assegura o Teorema 1, não significa que os números relativamente primos com mn sejam obtidos como produto dos números relativamente primos com m com os números relativamente primos com n. O que existe é uma correspondência biunívoca entre esses conjuntos, conforme ficou evidenciado na prova do referido teorema. A título de ilustrar essa observação vejamos o

EXEMPLO 3
Sejam $m = 6$ e $n = 5$, números primos entre si. Logo,
$\varphi(30) = \varphi(6 \times 5) = \varphi(6).\varphi(5) = 2 \times 4 = 8$.
Note que os o conjunto dos números inteiros positivos menores do que 6 e do que 5, relativamente primos com 6 e 5, respectivamente, são {1, 5} e {1, 2, 3, 4}. Enquanto que o conjunto dos números inteiros positivos menores do que 30 e relativamente primos com 30 é {1, 7, 11, 13, 17, 19, 23, 29}. Observe que nenhum número deste último conjunto, exceto o 1, é produto de dois números dos outros dois conjuntos anteriores.

EXERCÍCIO 3
Se p e $p + 2$ são dois primos, chamados de *primos gêmeos*, mostre que $\varphi(p + 2) = \varphi(p) + 2$.

O teorema anterior, juntamente com seu corolário, simplifica bastante o cálculo de $\varphi(n)$. Por exemplo, para calcular $\varphi(420)$ poderíamos fazer uso do Teorema calculando $\varphi(420) = \varphi(7 \times 60) = \varphi(7) \times \varphi(60)$. Mas, o uso do corolário anterior facilita ainda mais, pois $420 = 2^2 \times 3 \times 5 \times 7$ e como $2^2 = 4$, 3, 5 e 7 são dois a dois primos entre si, podemos escrever $\varphi(420) = \varphi(2^2)\ \varphi(3)\ \varphi(5)\ \varphi(7) = 2 \times 2 \times 4 \times 6 = 96$.

Uma aplicação direta do corolário anterior demonstra o seguinte:

TEOREMA 2
Seja $n = p_1^{r_1}.p_2^{r_2}...p_k^{r_k}$ a decomposição de n em fatores primos. Então

$$\varphi(n) = p_1^{r-1_1}.p_2^{r_2-1}...p_k^{r_k-1}(p_1-1).(p_2-1)....(p_k-1)$$

Demonstração

Como $p_1, p_2, ..., p_k$ são números primos distintos, então eles são dois a dois primos entre si. Logo, também quaisquer de suas potências são duas a duas primas entre si. Em particular, $p_i^{r_i}$ *e* $p_j^{r_j}$, para i ≠ j, são primos entre si. Usando o corolário do Teorema 1, podemos escrever

$$\varphi(n) = \varphi(p_1^{r_1}.p_2^{r_2}...p_k^{r_k}) = \varphi(p_1^{r_1}).\varphi(p_2^{r_2})\ldots\varphi(p_k^{r_k})$$

Mas, a Proposição 2 diz que se p é primo, então $\varphi(p^r) = p^{r-1}.((p-1)$. Logo, para cada j = 1, 2, ... , *k*, temos $\varphi(p_j^{r_j}) = p_j^{r_j-1}(p_j-1)$. Desse modo,

$$\begin{aligned}\varphi(n) &= p_1^{r_1-1}(p_1-1).p_2^{r_2-1}(p_2-1)....p_k^{r_k-1}(p_k-1)\\ &= p_1^{r-1_1}.p_2^{r_2-1}...p_k^{r_k-1}(p_1-1).(p_2-1)....(p_k-1)\end{aligned}$$

EXERCÍCIO 4

(a) Calcule φ(360)

(b) Encontre todos os inteiros positivos *n* para os quais φ(*n*) é ímpar.

O Teorema 3, a seguir, garante que a recíproca do Teorema 1 também é verdadeira.

TEOREMA 3

Se *m* e *n* são números naturais que não são primos entre si, então φ(*m.n*) ≠ φ(*m*).φ(*n*). Na realidade, neste caso, φ(*m*).φ(*n*) < φ(*m.n*).

Demonstração

Como MDC(*m, n*) > 1, então *m* e *n* possuem fatores primos em comum. Sejam $p_1, p_2, ..., p_t$ esses fatores primos comuns. Escrevemos

$m = p_1^{r_1}.p_2^{r_2}...p_t^{r_t}.a$ e $n = p_1^{s_1}.p_2^{s_2}...p_t^{s_t}.b$, onde MDC(*a, b*) = 1 e nem *a* nem *b* possui qualquer fator primo p_j, com j = 1, 2, 3, ..., t

[Por exemplo, $m = 2^2.3^2.5.91$ e $n = 2^2.3.5^2.121$, tem-se t = 3, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $r_1 = 3$, $r_2 = 2$, $r_3 = 1$, $a = 91$, $s_1 = 2$, $s_2 = 1$, $s_3 = 2$, $b = 121$]

Como $\varphi(m.n) = \varphi(p_1^{r_1+s_1}.p_2^{r_2+s_2}....p_t^{r_t+s_t}).\varphi(a).\varphi(b)$, pelo Teorema 2, temos que

$\varphi(p_1^{r_1+s_1}.p_2^{r_2+s_2}....p_t^{r_t+s_t}) = \varphi(p_1^{r_1+s_1}).\varphi(p_2^{r_2+s_2})....\varphi(p_t^{r_t+s_t})$. Como também temos que

$$\varphi(p_1^{r_1}.p_2^{r_2}...p_t^{r_t}) = \varphi(p_1^{r_1}).\varphi(p_2^{r_2})....\varphi(p_t^{r_t}) \quad \text{e}$$

$$\varphi(p_1^{s_1}.p_2^{s_2}...p_t^{s_t}) = \varphi(p_1^{s_1}).\varphi(p_2^{s_2})....\varphi(p_t^{s_t})$$

Pelo corolário da Proposição 2, para cada j = 1, 2, 3, ..., t, temos

$$\varphi(p_j^{r_j}).\varphi(p_j^{s_j}) < \varphi(p_j^{r_j+s_j})$$

Ao realizarmos a multiplicação de $\varphi(m)$ por $\varphi(n)$, aparecem os pares $\varphi(p_j^{r_j}).\varphi(p_j^{s_j})$ e ao calcular $\varphi(m.n)$, aparecem os fatores $\varphi(p_j^{r_j+s_j})$. Portanto, como $\varphi(a)$ *e* $\varphi(b)$ aparecem em ambas as expressões de $\varphi(m.n)$ e $\varphi(m).\varphi(n)$, segue que $\varphi(m).\varphi(n) < \varphi(m.n)$.

COLORÁRIO

Se *m* e *n* são inteiros positivos, então $\varphi(m.n) = \varphi(m).\varphi(n)$ se, somente se, *m* e *n* são primos entre si.

Demonstração

Suponha que existam *m* e *n* inteiros positivos com $\varphi(m.n) = \varphi(m).\varphi(n)$. Então a igualdade não pode acontecer se *m* e *n* não são primos entre si, pois, pelo Teorema 3, teríamos $\varphi(m).\varphi(n) < \varphi(m.n)$, contrariando a hipótese da igualdade.
Por outro lado, se *m* e *n* são primos entre si, pelo Teorema 1, $\varphi(m.n) = \varphi(m).\varphi(n)$.

Os resultados anteriores estabelecem propriedades multiplicativas da função φ sob certas condições. A pergunta que se impõe é se φ admite propriedades aditivas. Pela fato de um número inteiro puder se escrever como soma de dois outros inteiros de várias maneiras diferentes, contrariamente ao fato de ele ser decomposto em fatores primos de modo único – não se espera que φ tenha propriedades aditivas. Vejamos o exemplo que se segue para nos convencer dessa suspeita.

EXEMPLO 4

Sabemos que $\varphi(9) = 6$.
Enquanto que a decomposição $9 = 7 + 2$, fornece $\varphi(7) + \varphi(2) = 7 > \varphi(9) = 6$, a decomposição $9 = 6 + 3$ fornece $\varphi(6) + \varphi(3) = 4 < \varphi(9)$ e a decomposição $9 = 5 + 4$, fornece $\varphi(5) + \varphi(4) = 6 = \varphi(9)$.

Observação 2

Podemos afirmar, em caráter geral, que se *n* é um número primo, então para qualquer decomposição aditiva $p + q$ de *n* tem-se $\varphi(p) + \varphi(q) < \varphi(p + q) = \varphi(n)$. De fato, como $\varphi(n) = n - 1$, $\varphi(p) \leq p - 1$, $\varphi(q) \leq q - 1$, então $\varphi(p) + \varphi(q) \leq (p - 1) + (q - 1) < p + q - 1 = n - 1 = \varphi(n)$. Isto é, $\varphi(p) + \varphi(q) < \varphi(n) = \varphi(p + q)$.

EXERCÍCIO 5

Caracterize todos inteiros positivos *n* para os quais:
(a) $\varphi(n) = 2^k$ (b) $\varphi(n) = n/2$

2. A CONJECTURA DE GOLDBACH

Existe uma conjectura devida a Goldbach (*) de que qualquer inteiro par é a soma de dois números primos. Por exemplo: 10 = 7 + 3, 24 = 17 + 7, 36 = 31 + 5, 102 = 97 + 5 etc.

(*)A **conjectura de Goldbach**, proposta pelo matemático prussiano Christian Goldbach, é um dos problemas não resolvidos da Matemática, mais precisamente da Teoria dos Números, mais antigos atualmente. Ela diz que todo número par maior ou igual a 4 é a soma de dois primos. Por exemplo: 4 = 2 + 2; 6 = 3 + 3; 8 = 5 + 3; 10 = 3 + 7 = 5 + 5; 12 = 5 + 7; etc. Verificações por computador já confirmaram a conjectura de Goldbach para vários números. No entanto, a efetiva demonstração matemática ainda não ocorreu. O melhor resultado até agora foi dado por Olivier Ramaré em 1995: *todo número par é a soma de até 6 números primos*. Em 7 de junho de 1742, o matemático prussiano Christian Goldbach escreveu uma carta a Leonhard Euler, onde ele propôs à seguinte conjectura:
Todo inteiro par maior que 2 pode ser escrito como a soma de 3 números primos
Ele considerava o número 1 como sendo primo, que uma convenção posterior (e presente até hoje) abandonou. Uma visão moderna da Conjectura (e a mais aceita) é: *Todo inteiro par maior que 5 pode ser escrito como a soma de 3 números primos*. Euler, se interessado pelo problema, respondeu que a conjectura era equivalente à outra: *Todo inteiro par maior que 2 pode ser escrito como a soma de 2 números primos*. Euler adicionou, ainda, que estava absolutamente certo sobre isso, porém não era capaz de prová-lo. A versão de Euler é a mais conhecida e divulgada atualmente, também a mais aceita, por ser mais simples e abrangente. Para valores pequenos de *n*, a conjectura de Goldbach pode ser testada diretamente (método conhecido jocosamente pelos matemáticos como *força bruta e ignorância*). Em 1938, N. Pipping testou todos os números até 10^5.
(FONTE: http://pt.wikipedia.org/wiki/Conjectura_de_Goldbach)

Supondo verdadeira esta conjectura, podemos provar que dado um número n par, existem números primos r e s tais que $\varphi(r) + \varphi(s) = n$. De fato, se n é par então $n + 2$ é par. Sejam, portanto, r e s números primos tais que $r + s = n + 2$. Mas, $\varphi(r) = r - 1$ e $\varphi(s) = s - 1$, logo $\varphi(r) + \varphi(s) = (r + s) - 2 = (n + 2) - 2 = n$. Isto é, $\varphi(r) + \varphi(s) = n$.
Este resultado diz que se um número par n pode ser escrito como $\varphi(r) + \varphi(s)$ para r e s primos, então $n + 2$ não pode ser escrito como soma de dois números primos. E, nesse caso, não valeria a conjectura de Goldbach.

3. O TEOREMA DE EULER

O Pequeno Teorema de Fermat, estudado na Aula 07, afirma que se p é um número primo que não divide um inteiro a, então $a^{p-1} \equiv 1 \pmod{p}$. Euler (*) observou que $p - 1$ é exatamente igual a $\varphi(p)$, pois p é primo. Além disso, conseguiu uma generalização do Teorema de Fermat. Antes de precisar essa generalização, vamos precisar do seguinte

LEMA 2
Sejam x, m e k inteiros positivos, com k e m primos entre si. Seja r um inteiro tal que $x \equiv r \pmod{m}$ e $x \equiv r \pmod{k}$, então $x \equiv r \pmod{mk}$.
Demonstração

Pela hipótese, existem inteiros p e q tais que $x = qm + r$ e $x = pk + r$. Logo, $qm + r = pk + r$, donde $qm = pk$. Como m e k são primos entre si, essa igualdade só pode

acontecer se p e q são do tipo, q = q'm e p = p'k. Desse modo, x = q'mk + r. Ou seja, x ≡ r (mod mk).

TEOREMA 4 [Teorema de Euler (*)]
Sejam n e a inteiros positivos primos entre si. Então $a^{\varphi(n)} \equiv 1 \pmod{n}$.
Demonstração

Tomemos inicialmente $a = p^r$, com r inteiro positivo e p primo e não divisor de a. Pelo Pequeno Teorema de Fermat, temos

$$a^{p-1} \equiv 1 \pmod{p}.$$

De acordo com a propriedade básica VIII, das congruência, Aula 07, segue que

$$\left(a^{p-1}\right)^{p^{r-1}} \equiv 1 (\mathrm{mod}\ p)\text{. Ou seja, } a^{(p-1)p^{r-1}} \equiv 1 (\mathrm{mod}\ p).$$

Desse modo, existe um inteiro m tal que $\left(a^{p-1}\right)^{p^{r-1}} - 1 = mp$. Ou ainda,

$$a^{p^r - p^{r-1}} - 1 = mp.$$

Multiplicando ambos os membros da última igualdade por p^{r-1}, vem que

$$a^{p^r} - a^{p^{r-1}} = mp^r\text{, que implica em } a^{p^r} \equiv a^{p^{r-1}} (\mathrm{mod}\ p^r).$$

Como p^r e $a^{p^{r-1}}$ são primos entre si, pois p e a o são, então $a^{p^r - p^{r-1}} \equiv 1 (\mathrm{mod}\ p^r)$, que é o mesmo que escrever $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Para o caso geral, suponha que existe um inteiro positivo n tal que $a^{\varphi(n)}$ não seja congruente a 1 módulo n. Seja n_0 o menor inteiro com esta propriedade. Pelo caso anterior, n_0 não pode ser escrito como uma potência de um número primo. Logo, podemos escrever $n_0 = mk$, com m, k inteiros maiores do que 1 e primos entre si. Como $1 < m < n_0$, pela escolha de n_0, tem-se

$$a^{\varphi(m)} \equiv 1 \pmod{m} \text{ e } a^{\varphi(k)} \equiv 1 \pmod{n}.$$

Pela propriedade básica VIII, das congruência, Aula 07, podemos escrever

$$a^{\varphi(m).\varphi(k)} = [a^{\varphi(m)}]^{\varphi(k)} \equiv 1 \pmod{m} \quad \text{e} \quad a^{\varphi(m).\varphi(k)} = [a^{\varphi(k)}]^{\varphi(m)} \equiv 1 \pmod{k}$$

Mas, $\varphi(m).\varphi(k) = \varphi(mk) = \varphi(n_0)$. Logo, as igualdades anteriores podem ser escritas como

$$a^{\varphi(n_0)} \equiv 1 \pmod{m} \text{ e } a^{\varphi(n_0)} \equiv 1 \pmod{n}.$$

Como m e k são primos entre si, pelo Lema 2, segue que
$a^{\varphi(n_0)} \equiv 1 \pmod{mk} \equiv 1 \pmod{n_0}$, em contradição com a hipótese inicial.

(*) Leonhard Euler nasceu em 15 de Abril de 1707, em Basil, na Suíça. Foi sem dúvida o maior matemático do século dezoito. Com 886 trabalhos publicados, a maioria deles no final de sua vida, quando já estava completamente cego, Euler foi tão importante não apenas para a matemática, mas também a física, engenharia e astronomia, que termos como: Número de Euler, Números Eulerianos, Fórmula de Euler, significam coisas diferentes de acordo com o contexto.

Seu pai era um padre calvinista que nutria esperanças de que seu filho o precedesse no clericato. Ele ensinou a Euler a matemática. Quando seu filho entrou na Universidade de Basel, estudou Teologia e a língua Hebraica, e atendia a uma aula de uma hora por semana com Johannes Bernoulli. Ele fez amizade com Daniel e Nicolaus Bernoulli, e recebeu seu primeiro mestrado aos dezessete anos. Os Bernoullis, então, tiveram de persuadir seu pai a deixá-lo continuar com a carreira acadêmica. Aos dezenove anos, Euler recebeu menção honrosa por uma solução que enunciou a um problema posto pela academia de Paris. Mais tarde, ele ganhou o primeiro prêmio nesta mesma competição doze vezes.

Os Bernoullis conseguiram para Euler uma posição de pesquisa na Academia de São Petersburgo, mas em Medicina, sob o reinado de Catarina I. Porém, ela morreu logo após, e uma regime de condições caóticas se seguiu, com Euler passando à seção de matemática da Academia. Euler quis por muito tempo retornar à Europa, mas os constantes nascimentos de seus filhos o impediram. Porém, este foi um período extremamente produtivo para ele - era perigoso falar ou até mesmo sair às ruas, portanto Euler concentrou seus esforços na pesquisa e desenvolveu hábitos que manteve pelo resto de sua vida. Euler também escreveu livros didáticos para escolas russas, supervisionou o departamento de geografia do governo e ajudou a revisar o sistema de pesos e medidas. Ele permaneceu na Rússia até 1740, quando aceitou o convite de Frederico O Grande para entrar na academia de Berlin, onde passou os próximos 24 anos. Euler, porém, não era tão sofisticado quanto os outros membros da corte de Frederico e estes anos não foram totalmente agradáveis para ele. Porém, ele viveu relativamente bem e manteve uma casa em Berlin assim como uma fazenda. A situação na Rússia melhorou muito durante este período, e em 1766 Catarina A Grande o trouxe de volta a São Petersburgo. Ela deu a ele (e a seus 18 dependentes) uma casa mobiliada, e até mesmo um cozinheiro próprio.

Em 1735, Euler perdeu a visão de um de seus olhos, e, logo após seu retorno à Rússia, a visão em seu outro olho começou a deteriorar. Euler sempre teve uma memória excepcional, e era capaz de fazer enormes cálculos de cabeça, logo ele se preparou para sua futura cegueira aprendendo a escrever fórmulas em uma tábua e ditar matemática a seus filhos ou secretária. Ele foi cego pelos últimos 17 anos de sua vida, e durante este tempo sua produtividade somente aumentou.

Euler foi um cristão por toda a sua vida e frequentemente lia a Bíblia a sua família. Uma história sobre sua religião durante sua estada na Rússia envolve o dito filósofo ateu Diderot. Diderot foi convidado à corte por Catarina, mas tornou-se inconveniente ao tentar converter todos ao ateísmo. Catarina pediu a Euler que ajudasse, e Euler disse a Diderot, que era ignorante em matemática, que lhe daria uma prova matemática da existência de Deus, se ele quisesse ouvir. Diderot disse que sim, e, conforme conta De Morgan, Euler se aproximou de Diderot e disse, sério, em um tom de perfeita convicção: "(a + bn) / n = x, portanto, Deus existe". Diderot ficou sem resposta, e a corte caiu na gargalhada. Diderot voltou imediatamente à França.

Euler teve contribuições a várias áreas da ciência, incluindo dinâmica dos fluidos, teoria das órbitas lunares (marés), mecânica, "A teoria matemática do investimento" (seguros, anuidades, pensões), bem como essencialmente todas as áreas da matemática que existiam naquela época. Ele permaneceu são e alerta até o fim da sua vida, quando morreu de um derrame aos 76 anos. O trabalho ativo de Euler provocou uma tremenda demanda da academia de São Petersburgo, que continuou publicando seus trabalhos por mais de 30 anos após sua morte.

A memória de Euler era lendária, assim como seus poderes de concentração. Chamado de "Análise Encarnada", ele era capaz de recitar toda a Eneida de cor, e nunca foi atrapalhado por interrupções ou distrações, de modo que muito de seu trabalho foi realizado tendo suas crianças à sua volta. Ele era capaz de realizar cálculos prodigiosos de cabeça, uma necessidade depois que ele ficou cego. Seu matemático contemporâneo, Condorcet, conta uma história onde dois dos estudantes de Euler estavam calculando independentemente uma complicada série infinita, e chegaram a uma discussão depois de somarem dezessete termos, por uma diferença na qüinquagésima casa decimal. Euler resolveu a disputa fazendo a soma de cabeça. As funções e fórmulas de Euler são muito comuns na matemática. Duas das mais

famosas são: e^(ix) = cos(x) + i sin(x), e V - A + F = 2 para qualquer poliedro simples com Vértices, A arestas e F faces.
(FONTE: http://www.exatas.com/matematica/euler.html)

A seguir mostraremos exemplo do uso do Teorema de Euler.

EXEMPLO 5
Encontre o resto da divisão do número 39^{3602} por 14.
Solução

O número ao qual 39^{3602} é congruente é o resto solicitado. Ora, 39 e 14 são primos entre si e $\varphi(14) = \varphi(2.7) = \varphi(2).\varphi(7) = 1.6 = 6$ e $3602 = 600 \,.\, 6 + 2$. Pelo Teorema de Euler, temos $(39)^{\varphi(14)} = 39^6\, 39^2 \equiv 39^2 \pmod{14}$., donde $39^{3.600} \equiv 1 \pmod{14}$, o que nos dá $39^{3602} = 39^{3.600} \,.\, 39^2 \equiv 39^2 \pmod{14}$.
Como $39 \equiv 11 \pmod{14}$, segue que $39^2 \equiv 11^2 \pmod{14} = 121 \pmod{14} \equiv 9 \pmod{14}$.
Portanto, 9 é o resto solicitado.

EXERCÍCIO 6
Prove que o número $2222^{5555} + 5555^{2222}$ é divisível por 7.

Nessa altura cabe a seguinte pergunta:

Sendo $\varphi(n)$ um número par, para todo inteiro positivo $n > 2$, será que para todo número par k existe um inteiro positivo x tal que $\varphi(x) = k$?

A resposta é não. Por exemplo, para $k = 14$ a equação $\varphi(x) = 14$ não admite solução. Senão vejamos, na decomposição de x em seus fatores primos deve comparecer 7^r, para $r \geq 2$, pois $\varphi(x) = 2.7$. Desse modo, $\varphi(x) \geq (7 - 1).7^{r-1} = 6.\ 7^{r-1} \geq 6 \,.\, 7 = 42$. Portanto, a equação $\varphi(x) = 14$ não admite solução.

O exemplo a seguir ilustra uma aplicação interessante do Teorema de Euler.

EXEMPLO 6
Se *a* e *n* são primos entre si, então $x = ba^{\varphi(n)-1}$ é a única solução módulo *n* da congruência linear $ax \equiv b \pmod{n}$.
Solução

De fato, $ax = a(ba^{\varphi(n)-1}) = ba^{\varphi(n)}$. Mas, $a^{\varphi(n)} \equiv 1 \pmod{n}$, pelo Teorema de Euler. Logo, $ba^{\varphi(n)} \equiv b \pmod{n}$, donde o afirmado.
Agora suponha x e x' duas soluções módulo *n*. Isto é,

$$ax \equiv b \pmod{n} \quad \text{e} \quad ax' \equiv b \pmod{n}.$$

Logo, $ax \equiv ax' \pmod{n}$, donde $x \equiv x' \pmod{n}$, pois $MDC(a, n) = 1$.

EXEMPLO 7

Encontre todas as soluções módulo 35 da congruência linear $6x \equiv 13 \pmod{35}$.
Solução

Como 6 e 35 são primos entre si, pelo exemplo anterior, temos

$$x = 13.6^{\varphi(35)-1} = 13.6^{23} = 13.6^{20}.6^3 = 13.(6^2)^{10}.6^3 \equiv 13.1.6 \pmod{35} =$$

$$= 78 \pmod{35} = 8 \pmod{35}.$$ Logo, $x \equiv 8 \pmod{35}$ é a única solução da equação inicial.

4. EXERCÍCIOS

1) Mostre que φ não é uma função crescente. No entanto, a restrição de φ ao conjunto dos números primos é crescente.

2) Encontre o algarismo das unidades do número $3^{10.007}$.

3) Prove que se m divide n, então $\varphi(m)$ divide $\varphi(n)$.
[Sugestão: Se $p_1^{r_1}.p_2^{r_2}...p_t^{r_t}$ é a decomposição de m em seus fatores primos, conclua que $n = p_1^{s_1}.p_2^{s_2}...p_t^{s_t}.a$, onde $s_k \geq r_k$ e MDC$(a, p_i) = 1$, para i = 1, 2, 3,..., k.]

4) Encontre os valores x para os quais $\varphi(x) = 16$. O mesmo para $\varphi(x) = 18$.

5) Seja p um número primo. Mostre que a equação $\varphi(x) = 2p$, tem solução se, e somente, $2p + 1$ é um número primo.
[Sugestão: Para a recíproca, suponha que a equação tenha um número composto x como solução e conclua que $x = p^r$, com $r \geq 2$]

6) Calcule $\varphi(n)$ para os seguintes valores de n:
   a. $n = 694\,575$
   b. $n = 1\,308\,736$

7) Faça uma tabela dos valores de $\varphi(n)$ para $n \leq 36$.

8) Para todo número par $n \leq 12$, encontre dois valores de x tais que $\varphi(x) = n$. Mostramos anteriormente que a equação $\varphi(x) = 14$ não tem solução. Portanto, $n = 14$ é o menor valor de n par tal que a equação $\varphi(x) = n$ não admite solução.

6. RESUMO

Nesta aula introduzimos a função φ de Euler como sendo a função que conta os números positivos, relativamente primos com um inteiro n, e menores do que n. Isso nos permitiu estabelecer um teorema, devido a Euler, o qual generaliza o Pequeno Teorema de Fermat, estudado na Aula 07.

7. REFERÊNCIAS

[1] Burton, David M. – Elementary Number Theory. The McGraw-Hill Companies, Inc. New York. USA. 1998

[2] Coutinho, S. C. – Números Inteiros e Criptografia RSA. Instituto de Matemática Pura e Aplicada – IMPA & Sociedade Brasileira de Matemática – SBM. Rio de Janeiro. 1997

[3] Hefez, Abramo – Elementos de Aritmética. Sociedade Brasileira de Matemática. Rio de Janeiro. 2005

[4] Oliveira, José Plínio, de – Introdução à Teoria dos Números. Publicação IMPA. Rio de Janeiro. 2000

AULA 10 – Sequências de Fibonacci

Apresentação

Nesta aula, estudaremos as Seqüências de Fibonacci, assim denominadas em homenagem ao italiano Leonardo de Pisa, mais conhecido como Fibonacci, que significa filho de Bonacci. Ele nasceu em 1180 na cidade de Pisa, na época do início da construção da famosa Torre de Pisa, e introduziu na Europa o sistema de numeração hindu-arábico através do seu famoso livro Líber Abaci (1202). Fibonacci é considerado o maior matemático da Idade Média. Seu livro *Líber Abaci* contém um problema famoso sobre coelhos, cuja solução é agora conhecida como a Seqüência de Fibonacci. Surpreendentemente, os números de Fibonacci, isto é, os números que comparecem na Seqüência de Fibonacci, servem para representar modelos da natureza, como o número de espirais em determinadas rosas, frutas, como os girassóis, a pinha, o abacaxi etc.

Tente entender tudo que está sendo explicado na aula. Estude com caneta e papel ao lado. Leia com atenção. Se for preciso, leia várias vezes uma linha ou um parágrafo. Seja paciente e procure ter certeza que você entendeu o que (e por que) está fazendo.

Objetivos

Com esta aula espera-se que você possa:

1) Identificar uma sequência de Fibonacci*;*

2) Perceber relações entre números de Fibonacci;

3) Usar seqüências de Fibonacci para resolver problemas práticos;

1. A SEQÜÊNCIA DE FIBONACCI

]

Figura 1 - Leonardo de Pisa (1180-1250)

OS NÚMEROS DE FIBONACCI

Fibonacci - que significa filho de Bonacci- era o pseudônimo de Leonardo de Pisa, que é considerado o maior matemático da Idade Média. Como mercador, viajou pelo Oriente. No seu regresso, escreveu os livros *Liber Abaci (*1202) e *Practica Geometricae* (1220*).* No primeiro livro, descreveu fatos de aritmética e álgebra recolhidos durante sua viagem. No segundo, descreveu o que tinha descoberto na geometria e na trigonometria, [3] página 138.

O *Liber Abaci* foi um instrumento que permitiu difundir na Europa ocidental o sistema de numeração hindu-árabe, que era usado ocasionalmente já alguns séculos antes de Leonardo de Pisa, e que foi trazido pelos mercadores, embaixadores, eruditos, peregrinos e soldados vindo da Espanha e do Oriente, [3] página 139.

Fibonacci ficou conhecido entre nós não exatamente por seus livros, mas porque no século XIX o matemático francês F. Edouard A. Lucas, na sua coleção *Récreations mathématique* (4 volumes, Gauthier-Villars, Paris 1891-1896; reeditado em Paris 1960), ligou o nome de Fibonacci à seqüência que aparece num problema do livro Liber Abaci. O problema, relacionado com o número de casais de coelhos obtidos a partir de um único casal, era:

Quantos casais de coelhos podem ser produzidos a partir de um único casal durante um ano se:

(a) um casal de coelhos é colocado num cercado;
(b) Os coelhos precisam de dois meses até chegar à idade adulta e poder reproduzir-se;

(c) cada casal origina um novo casal em cada mês, o qual se torna fértil a partir do segundo mês;
(d) nenhum coelho mais pode vir de fora, nenhum coelho pode sair do cercado e não ocorrem mortes.

Nessas condições, um casal nasce no primeiro mês, totalizando-se assim 2 casais. Durante o segundo mês, o casal original produz um novo casal. Um mês depois, o casal original e o que nasceu imediatamente após o seu acasalamento, produzem novos casais. Nessa altura, já existem 3 casais adultos e dois casais filhotes. E, assim por diante. Veja o quadro a seguir:

Quadro 1 – O crescimento dos casais de Coelhos

Mês	Casais Adultos	Casais Jovens	TOTAL
1	1	1	2
2	2	1	3
3	3	2	5
4	5	3	8
5	8	5	13
6	13	8	21
7	21	13	34
8	34	21	55
……	……	……	……
……	……	……	……

A seqüência de Fibonacci é constituída pelos totais de casais, isto é, os números

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233,.....

Algumas perguntas ocorrem naturalmente:

- É possível encontrar uma relação simples entre os termos da seqüência de Fibonacci?
- Que relação existe entre os termos consecutivos da seqüência de Fibonacci?
- Quantos casais de coelhos haverá no final de doze meses?
- É possível encontrar uma fórmula simples para a soma dos n primeiros termos da seqüência de Fibonacci?
- Existe uma fórmula para descrever os termos da seqüência de Fibonacci?

Essas perguntas serão abordadas nas próximas seções.

2. PROPRIEDADES ELEMENTARES

2.1 A Igualdade Fundamental

Vamos denotar por (f_n) a seqüência de Fibonacci e seus termos por:

$f_1 = 1, \quad f_2 = 1, \quad f_3 = 2, \quad f_4 = 3, \quad f_5 = 5, \quad f_6 = 8, \quad f_7 = 13, \ .....$

Com essa notação, a seqüência de Fibonacci exibe uma propriedade interessante:

$f_3 = f_1 + f_2$; $f_4 = f_2 + f_3$; $f_5 = f_3 + f_4$; $f_6 = f_4 + f_5$

De uma maneira geral, os termos de uma seqüência de Fibonacci satisfazem a relação:

$f_1 = 1$, $f_2 = 1$, $f_n = f_{n-1} + f_{n-2}$, para $n \geq 3$.

Isto é, cada termo da seqüência, a partir do terceiro, é a soma dos dois imediatamente inferiores. Desse modo, descreve-se a seqüência de Fibonacci como uma seqüência recursiva, ou seja, uma seqüência na qual todo termo pode ser representado como uma combinação linear dos termos precedentes. Isto é,

$f_1 = 1$, $f_2 = 1$, $f_n = f_{n-1} + f_{n-2}$, para $n \geq 3$.

A seqüência de Fibonacci é a primeira seqüência recursiva conhecida na literatura matemática (Por volta de 1634, a partir dos trabalhos de Albert Girard [1], página 287).

EXEMPLO 1
Numa faixa 1 x 10, veja a figura 2, a seguir, cada quadrado é pintado ou de azul ou de vermelho, mas dois quadrados adjacentes não podem ser pintados de azul.

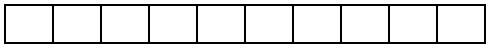

Figura 2 – Faixa de quadrados 1 x 10

De quantas maneiras distintas podemos realizar a pintura?
Solução

Certamente existem muitas maneiras diferentes de realizarmos a pintura. Mas, como contar todas essas maneiras?
Construamos, mentalmente, uma faixa menos complicada, com um número menor de quadrados.
Começamos pensando na faixa tendo um só quadrado. Neste caso, existem duas maneiras de pintar: ou pintamos o quadrado de azul (A) ou pintamos o quadrado de vermelho (V).

Se a faixa possui dois quadrados. Neste caso, se o primeiro quadrado for pintado de vermelho (V), temos duas possibilidades para pintar o segundo quadrado: azul (A) ou vermelho (V). Se o primeiro quadrado for pintado de azul (A), só podemos pintar o segundo de vermelho (V). Portanto, com as regras dadas, podemos pintar uma faixa com dois quadrados de três modos distintos:

VA;
VV;
AV.

Se a faixa possui três quadrados. Neste caso, se o primeiro quadrado for pintado de vermelho (V), temos três possibilidades para pintar os dois quadrados seguintes VA, VV e AV . Se o primeiro quadrado for pintado de azul (A), temos duas possibilidades

para pintar os dois quadrados seguintes: VV e VA. Portanto, com as regras dadas, podemos pintar de cinco modos diferentes uma faixa com três quadrados:

VVA;
VVV;
VAV;
AVV;
AVA.

E se a faixa possui quatro quadrados? Seguimos o raciocínio anterior. Para isso, escolhemos a pintura do primeiro quadrado e pintamos os quadrados restantes olhando para as pinturas já feitas. Se pintarmos o primeiro quadrado de vermelho (V), com as regras dadas, os três quadrados restantes podem ser pintados de cinco maneiras distintas, como se fosse o caso de a faixa ter dois quadrados, e teremos as seguintes pinturas possíveis:

VVVA;
VVVV;
VVAV;
VAVV;
VAVA

Se pintarmos o primeiro quadrado de azul (A), de acordo com as regras dadas, o próximo quadrado só pode ser pintado de vermelho (V) e os dois quadrados restantes podem ser pintados de dois modos distintos, como se fosse o caso da faixa ter dois quadrados. Assim, a pintura seria:

AVVA;
AVVV;
AVAV.

Portanto, no caso de a faixa ter quatro quadrados, podemos pintá-la de 5 + 3 = 8 modos distintos.

Para o caso da faixa ter cinco quadrados, usamos o mesmo argumento do caso da faixa ter quatro quadrados. Ou seja, se pintarmos o primeiro quadrado de vermelho (V), com as regras dadas, existem 8 possibilidades para efetuar a pintura dos quatro quadrados restantes. E se o primeiro quadrado for pintado de azul (A), com as regras dadas, o segundo só pode ser pintado de vermelho (V) e os três restantes de 5 modos distintos, dando um total de 8 + 5 = 13 possibilidades de pintura.

Portanto, seguindo este raciocínio, o número de maneiras distintas de pintarmos uma faixa de comprimento 1 x n é dada, de acordo com o número de quadrados, *n*, pela seqüência de números 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ..., onde cada termo é a soma dos dois termos precedentes. Esta é a Seqüência de Fibonacci. Portanto, a resposta, para $n = 10$, é 144.

EXERCÍCIO 1

Seja $\{f_1 = 1,\ f_2 = 1,\ f_3 = 2,\ f_4 = 3,\ f_5 = 5,\ f_6 = 8,\ f_7 = 13,\ f_n, \ldots\ldots\}$ a seqüência de Fibonacci, satisfazendo de uma maneira geral: $f_n = f_{n-1} + f_{n-2}$, para $n \geq 3$.
Verifique que os termos $f_3, f_6, f_9, \ldots$ são todos números pares.

[Sugestão: Usando que $f_n = f_{n-1} + f_{n-2}$, para $n \geq 3$, mostre que $f_{n+3} \equiv f_n \pmod 2$]

2.2 A Soma dos primeiros n termos da seqüência de Fibonacci

A soma dos n primeiros termos da seqüência de Fibonacci tem uma fórmula fácil de gravar, dada na

PROPOSIÇÃO 1
Sejam $f_1 = 1$, $f_2 = 1$, $f_n = f_{n-1} + f_{n-2}$, para $n \geq 3$. A soma, S_n, dos primeiros *n* termos da seqüência de Fibonacci é dada por:

$$S_n = f_1 + f_2 + f_3 + ... + f_n = f_{n+2} - 1$$

Demonstração

Começamos escrevendo a igualdade fundamental: $f_{k+2} = f_k + f_{k+1}$, para $k \geq 1$.
Daí segue que $f_k = f_{k+2} - f_{k+1}$. Agora, fazendo k = 1, 2, 3, 4,..., n e somando membro a membro, obtemos

$$\begin{aligned} S_n = f_1 + f_2 + f_3 + ... + f_n &= (f_3 - f_2) + (f_4 - f_3) + (f_5 - f_4) + ... + (f_{n+2} - f_{n+1}) = \\ &= (f_3 - 1) + (f_4 - f_3) + (f_5 - f_4) + ... + + (f_{n+1} - f_n) + (f_{n+2} - f_{n+1}) \\ &= f_{n+2} - f_2 = f_{n+2} - 1. \end{aligned}$$

Veja que os termos intermediários se cancelam, resultando somente os termos extremos: $f_{n+2} - 1$.

EXEMPLO 2
Mostre que a soma de quaisquer 10 termos consecutivos da seqüência de Fibonacci é igual a 11 vezes o sétimo desses termos.
Solução

Considere os 10 termos da seqüência Fibonacci como sendo:

a, b, a + b, a + 2b, 2a + 3b, 3a + 5b, 5a + 8b, 8a + 13b, 13a + 21b, 21a + 34b.

O sétimo termo da seqüência é $5a + 8b$ e a soma dos 10 termos é igual a
$S = 55a + 88b = 11(5a + 8b)$, com queríamos mostrar.

EXERCÍCIO 2
Sejam $f_1 = 1$, $f_2 = 1$, $f_n = f_{n-1} + f_{n-2}$, para $n \geq 3$.Verifique que a seguinte igualdade: $f_1 + f_2 + f_3 + f_4 + f_5 + f_6 + f_7 + f_8 = f_{10} - 1$.

2.3 Termos Consecutivos da Seqüência de Fibonacci são Relativamente Primos

Observando-se os números iniciais da seqüência de Fibonacci, podemos notar que termos consecutivos (f_1 e f_2; f_2 e f_3; f_3 e f_4; assim por diante) são relativamente primos (i.e. têm Máximo Divisor Comum igual a 1).
Uma pergunta ocorre naturalmente:

Isso se verifica para todo n? Isto é, f_n e f_{n-1} são relativamente primos?

A resposta é afirmativa:

Teorema 1
Na seqüência, (f_n), de Fibonacci, temos que MDC $(f_n, f_{n-1}) = 1$, para todo $n \geq 2$.
Demonstração

O caso em que n for igual a 1 ou 2 é trivialmente verdadeiro. Para $n \geq 3$, faremos um argumento por redução ao absurdo. Isto é, supõe-se que MDC(f_n, f_{n-1}) seja um inteiro d maior do que 1 e vamos chegar a uma contradição. Assim, vamos supor, pelo Princípio do Menor Inteiro, que existe n o menor inteiro positivo tal que MDC$(f_n, f_{n-1}) = d > 1$. Nesse caso, d divide f_n e d divide f_{n-1}. Como $f_n = f_{n-1} + f_{n-2}$, para $n \geq 3$, segue que d divide f_{n-2}, contrariando a escolha de n.

Uma pergunta ocorre naturalmente:

Como $f_3 = 2$, $f_5 = 5$, $f_7 = 13$ e $f_{11} = 89$ são todos primos, podemos concluir que f_n é primo sempre que n seja primo?

A resposta é não.
Para ilustrar, veja o contra-exemplo: 19 é primo, mas, no entanto, $f_{19} = 4181 = 37 \times 113$ é um número composto.
Você pode encontrar outro contra-exemplo?

EXEMPLO 3
Verifique se os números de Fibonacci f_{13} e f_{17} são primos.
Solução

Usando a relação $f_n = f_{n-1} + f_{n-2}$, para $n \geq 3$, temos: $f_1 = 1$, $f_2 = 1$, $f_3 = 2$, $f_4 = 3$, $f_5 = 5$, $f_6 = 8$, $f_7 = 13$, $f_8 = 21$, $f_9 = 34$, $f_{10} = 55$, $f_{11} = 89$, $f_{12} = 144$, $f_{13} = 233$, $f_{14} = 377$, $f_{15} = 610$, $f_{16} = 987$, $f_{17} = 1597$.
Agora, basta observar que: $f_{13} = 233$ é primo, pois não é divisível por qualquer inteiro positivo que seja maior do que 1 e menor do que $\sqrt{233} \cong 15{,}264$. Do mesmo modo, $f_{17} = 1597$ é primo, pois não tem qualquer divisor entre 1 e $\sqrt{1597} \cong 39{,}96$.

EXERCÍCIO 3
Calcule:
(a) MDC (f_{15}, f_{20}) (b) MDC (f_{16}, f_{24}) .

Não se conseguiu ainda determinar quais são todos os números inteiros positivos n para os quais f_n seja primo. Você pode resolver esse problema e tornar-se um matemático conhecido! Também não se sabe ainda se o número de primos na seqüência de Fibonacci é infinito. Outro problema intrigante! Você pode também ficar famoso se conseguir resolvê-lo!

2.4 O Algoritmo da Divisão e a Seqüência de Fibonacci

É um fato conhecido, estudado na Aula 05, "O Máximo Divisor Comum, O Mínimo Múltiplo Comum e as Equações Diofantinas Lineares", que o Máximo Divisor Comum de dois inteiros positivos pode ser calculado a partir do Algoritmo da Divisão, depois de um número finito de divisões. Por exemplo, para calcular o MDC(32,12) começamos dividindo 32 por 12:

$32 = 2 \times 12 + 8$, onde 8 é o resto da divisão e 2 é o quociente.

Em seguida, fazemos a divisão do quociente pelo resto da divisão anterior:

$12 = 1 \times 8 + 4$.

Finalmente, dividimos 8 por 4: $8 = 2 \times 4 + 0$.
Como o resto da última divisão é zero, dizemos que MDC(32,12) = 4. Nesse caso, foi preciso 3 divisões para encontrar o Máximo Divisor Comum.

Por uma escolha conveniente dos inteiros, o número de divisões pode ser arbitrariamente grande.
Você é capaz de dar exemplos dessa situação?

Nessa altura, uma pergunta aparece naturalmente:

Dado um inteiro positivo n, existem inteiros positivos a e b tais que, para se calcular MDC(a, b) usando o Algoritmo da Divisão necessita-se de exatamente n divisões?

A resposta é afirmativa e foi dada, em 1844, por Gabriel Lamé (1825-1871), um matemático francês. Lamé, ao responder a pergunta, descobriu uma surpreendente ligação entre os números de Fibonacci e o Algoritmo da Divisão. A resposta foi dada tomando $a = f_{n+2}$ e $b = f_{n+1}$. Nesse caso, o uso do Algoritmo da Divisão para a obtenção do MDC(f_{n+2}, f_{n+1}) leva-nos ao sistema de equações:

$$
\begin{aligned}
f_{n+2} &= 1 \times f_{n+1} + f_n \\
f_{n+1} &= 1 \times f_n + f_{n-1} \\
f_n &= 1 \times f_{n-1} + f_{n-2} \\
&\cdots\cdots\cdots\cdots \\
f_4 &= 1 \times f_3 + f_2 \\
f_3 &= 2 \times f_2 + 0
\end{aligned}
$$

Do sistema de equações acima, fica claro que MDC(f_{n+2}, f_{n+1}) = f_2 = 1 e que o número de divisões é n.

Uma conseqüência surpreendente é dada na seguinte

Proposição 2
O número de divisões necessárias para achar o Maior Divisor Comum de dois inteiros positivos, *a* e *b*, usando o Algoritmo da Divisão, não excede a cinco vezes o número de algarismos (na base decimal) do menor número.

Demonstração

Seja $a \leq b$, com o número a possuindo k algarismos na base dez. Nesse caso, $a < 10^k$. Se, usando o Algoritmo da Divisão para calcular o MDC(a, b), necessitamos de n divisões, então $a \geq f_{n+1}$. Portanto, de acordo com o argumento anterior de Lamé, $10^k > f_{n+1}$.

Usando indução, podemos mostrar que $f_m > (8/5)^{m-2}$, para todo m > 2, e, portanto

$$10^k > (8/5)^{n-1}$$

Elevando cada lado a potência 5, obtemos

$$10^{5k} > [(8/5)^5]^{n-1} > 10^{n-1}$$

Assim, 5k > n-1, e, como k é inteiro, n ≤ 5k, como queríamos.
Sobre essa questão uma interessante referência em português é [2].

Outro fato interessante a respeito da seqüência de Fibonacci é:

PROPOSIÇÂO 3
Os termos da seqüência, (f_n), de Fibonacci satisfazem a identidade:

$f_{m+n} = f_{m-1} f_n + f_m f_{n+1}$

Demonstração

Um exemplo é fácil de achar. Senão vejamos, para calcular f_9 basta aplicar a identidade:
$f_9 = f_{6+3} = f_5 f_3 + f_6 f_4 = 5 \times 2 + 8 \times 3 = 34$.
Mas, como sabemos se a identidade acima é válida para todo inteiro m e n?
Para responder a essa questão, vamos fazer uma demonstração por indução sobre n. Para isso, fixemos m. Se $n = 1$, a identidade torna-se

$$f_{m+1} = f_{m-1} f_1 + f_m f_2 = f_{m-1} .1 + f_m .1 = f_{m-1} + f_m ,$$

que é verdadeira, por ser a relação fundamental da seqüência de Fibonacci. Suponha que a identidade acima seja verdadeira quando n é um dos inteiros: 1, 2, 3, 4,..., k. Assim, tem-se

$$f_{m+k} = f_{m-1} f_k + f_m f_{k+1} \text{ e também } f_{m+(k-1)} = f_{m-1} f_{k-1} + f_m f_k$$

Somando-se as duas igualdades e aplicando-se a igualdade fundamental mostra-se que $f_{m+(k+1)} = f_{m-1} f_{k+1} + f_m f_{k+2}$. O que conclui a prova.

EXEMPLO 4
Mostre a seguinte identidade: $f_{m+3} = 3f_{m+1} - f_{m-1}$, para $m \geq 2$.
Solução

Da Proposição 3, temos $f_{m+3} = f_{m-1} f_3 + f_m f_4 = 2f_{m-1} + 3f_m$, pois $f_3 = 2$ e $f_4 = 3$. Agora, usando a relação $f_m = f_{m-1} + f_{m-2}$, reescrevemos a última expressão obtida como:
$f_{m+3} = 2f_{m-1} + 3f_m = 2f_{m-1} + 2f_m + f_m = 2(f_{m-1} + f_m) + f_m = 2f_{m+1} + f_m = 2f_{m+1} + (f_{m+1} - f_{m-1}) =$
$= 3f_{m+1} - f_{m-1}$, como queríamos mostrar.

ATIVIDADE 4

Demonstre a identidade de Cassini:

O quadrado de qualquer termo da seqüência de Fibonacci difere do produto dos termos adjacentes por 1 ou -1. Isto é, $f_{n-1} f_{n+1} - f_n^2 = (-1)^n$

[Sugestão: Em vez de fazer contas, verifique o resultado surpreendente

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$$

e use o fato de que para duas matrizes quadradas A e B, de mesma ordem, tem-se det(AB) = det(A).det(B)]

Nota: Jean-Dominique Cassini descobriu essa identidade em 1680, veja J.D. Cassini, *Une nouvelle progression de nombres,* Histoire de l'Academie Royale des Sciences, Paris, 1 (1733) 496-201.

2.5 O Teorema de Lucas

Em 1876, o matemático francês F. Edouard A. Lucas provou que o Máximo Divisor Comum de dois números de Fibonacci era outro número de Fibonacci. Mais precisamente,

Teorema 2 (Lucas)

Se (f_n) é a seqüência de Fibonacci, então MDC $(f_m, f_n) = f_{MDC(m, n)}$.

Antes de demonstrarmos o Teorema de Lucas, vamos provar os seguintes lemas:

Lema 1

Para m, n inteiros maiores do que ou iguais a 1, f_{mn} é divisível por f_m.

Demonstração

A prova é por indução sobre n.

Para n = 1 o resultado é verdadeiro, pois $f_{mn} = f_m$. Suponha que para n = 1, 2, 3..., k, f_{mn} seja divisível por f_m. O caso $(n+1)$ é verificado usando a fórmula fundamental:

$$f_{m\,(k+1)} = f_{m(k-1)} f_m + f_{mk} f_{m+1}$$

Como, por hipótese de indução, f_m divide f_{mk}, o lado direito da expressão acima é divisível por f_m, e, portanto, $f_{m\,(k+1)}$ é divisível por f_m.

Lema 2
Se m e n são inteiros positivos ($m \geq n$) com $m = qn + r$, $0 \leq r < n$, então MDC(f_m, f_n) = MDC(f_n, f_r).
Demonstração

Pela igualdade fundamental temos:

MDC(f_m, f_n) = MDC(f_{qn+r}, f_n) = MDC($f_{q(n-1)}\, f_r + f_{qn}\, f_{r+1}$, f_n).

Usando o Lema 1 e o fato de que MDC($a+b$, c) = MDC(a, c), sempre que c dividir b temos

$$MDC(f_{q(n-1)}f_r + f_{qn}f_{r+1},\ f_n) = MDC(f_{q(n-1)}f_r,\ f_n)$$

Agora, vamos mostrar que d = MDC(f_{qn-1}, f_n) = 1. As relações: d divide f_n e f_n divide f_{qn}, implicam que d divide f_{qn}. Portanto, d é um inteiro positivo que divide dois termos consecutivos, f_{qn} e f_{qn-1}, da seqüência de Fibonacci. Logo d = 1. Por outro lado,

$$MDC(f_m,\ f_n) = MDC(f_{q(n-)1}f_r,\ f_n) = MDC(f_r,\ f_n)$$

A última igualdade decorre do fato: sempre que MDC(a,b) = 1, temos MDC(a, bc) = MDC(a,c). O que finaliza a demonstração.

Agora, estamos em condições de demonstrar o Teorema de Lucas.

Demonstração do Teorema de Lucas

Suponha que m ≥ n. Aplicando o Algorítmo da Divisão para m e n, obtemos o seguinte sistema de equações :

$$\begin{aligned}
&m = q_1 n + r_1,\ 0 \leq r_1 < n \\
&n = q_2 r_1 + r_2,\ 0 \leq r_2 < r_1 \\
&r_1 = q_3 r_2 + r_3,\ 0 \leq r_3 < r_2 \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&r_{n-2} = q_n r_{n-1} + r_n,\ 0 \leq r_n < r_{n-1} \\
&r_{n-1} = q_{n+1} r_n + 0,
\end{aligned}$$

De acordo com o Lema 2, temos

$$\mathbf{MDC(f_m, f_n) = MDC(f_n, f_{r_1}) = ... = MDC(f_{r_n}, f_{r_{n-1}})}$$

Como r_n divide r_{n-1}, o Lema 1 garante que f_{r_n} divide $f_{r_{n-1}}$. Portanto, temos que:
$\mathbf{MDC(f_{r_n}, f_{r_{n-1}}) = f_{r_n}}$. Mas, r_n sendo o último resto não nulo no Algorítmo Euclides para m e n, ele é o MDC(m, n). O que encerra a prova.

2.5 A Fórmula de Binet

A pergunta:

"Existe uma fórmula geral que expresse o n-ésimo termo da seqüência de Fibonacci?"

tem resposta afirmativa. A fórmula foi descoberta em 1718 pelo matemático francês De Moivre. Mas, a fórmula ficou conhecida pelo nome de *Fórmula de Binet*, em homenagem ao matemático francês que a resdescobriu mais de um século depois, em 1843. Antes de apresentarmos a fórmula de Binet, vamos fazer algumas observações.

A seqüência de Fibonacci não é a única seqüência que satisfaz a fórmula recursiva

$$\mathbf{f_{n+2} = f_n + f_{n+1}} \qquad (*)$$

De fato, a chamada seqüência de Lucas

1, 3, 4, 7, 11, 18, ...

também satisfaz a relação (*). Na verdade, existe uma infinidade de seqüências satisfazendo a relação (*). O lema seguinte mostra como podemos produzir novas soluções de (*), isto é, outras seqüência satisfazendo a relação
$\mathbf{f_{n+2} = f_n + f_{n+1}}$ (*).

Lema 3
(a) Se A = (a_1, a_2, a_3,...) é uma solução de (*) e c é um número real qualquer, então a seqüência

$$c\mathrm{A} = (ca_1, ca_2, ca_3, \ldots)$$

é também solução de (*).
(b) Se as seqüências A = (a_1, a_2, a_3,...) e B = (b_1, b_2, b_3,...) satisfazem (*), então a soma

$$\mathrm{A} + \mathrm{B} = (a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots)$$

também satisfaz a relação (*)

Demonstração

(a) Se A satisfaz a relação fundamental (*), temos que $a_{n+2} = a_n + a_{n+1}$. Agora multiplicando por c ambos os membros da última relação, temos $ca_{n+2} = ca_n + ca_{n+1}$. Portanto a sequência cA é uma solução de (*).
(b) Se as seqüências A e B satisfazem (*), então $a_{n+2} = a_n + a_{n+1}$ e $b_{n+2} = b_n + b_{n+1}$. Assim, somando membro a membro as duas igualdades, obtemos $a_{n+2} + b_{n+2} = (a_n + b_n) + (a_{n+1} + b_{n+1})$. O que mostra que a seqüência A + B satisfaz (*).

TEOREMA 3 (A Fórmula de Binet)
O *n*-ésimo termo da seqüência de Fibonacci é dado pela fórmula

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

Demonstração

É interessante observar que, uma seqüência extremamente fácil de definir recursivamente tenha, para cada termo, uma fórmula complicada. Observe que, apesar de não ser fácil visualizar, o lado direito da fórmula acima é um inteiro!

Observe que, se r é a raiz positiva da equação $x^2 = x + 1$, então $r^2 = r + 1$. Logo, $r = \frac{1+\sqrt{5}}{2}$.

Multiplicando cada lado de $r^2 = r + 1$ por r^n, obtemos

$$r^{n+2} = r^{n+1} + r^n,$$

para todo n = 1, 2, 3, 4,....

Assim, $(r, r^2, r^3,....)$ é uma seqüência satisfazendo (*). Seja $u = 1 - r = \frac{1-\sqrt{5}}{2}$ a outra solução da equação $x^2 = x + 1$. Logo, $(u, u^2, u^3,....)$ é uma seqüência satisfazendo (*).
Pelo Lema 3, a seqüência $(r - u, r^2 - u^2, r^3 - u^3,...)$ satisfaz (*). Mas, os dois primeiros termos (pois r e *u* são soluções de $x^2 = x + 1$) são iguais, pois

$$r^2 - u^2 = (r - u)(r + u) = 1.(r - u) = r - u,$$

e, portanto, a seqüência $\frac{r^n - u^n}{r - u} = a_n$, com n = 1, 2, 3, ... Isto é, $a_1 = a_2 = 1$, e pelo Lema 3, satisfaz $a_{n+2} = a_n + a_{n-1}$, tem de ser a seqüência de Fibonacci. E $\frac{\mathbf{r^n - u^n}}{\mathbf{r - u}}$ é exatamente o valor da fórmula de Binet, uma vez que $r^n = \left(\frac{1+\sqrt{5}}{2}\right)^n$, $u^n = \left(\frac{1-\sqrt{5}}{2}\right)^n$ e $r - u = \sqrt{5}$. Isso conclui a prova.

Observe, a partir da fórmula de Binet, que

f_n é aproximadamente igual a $\frac{\mathbf{r^n}}{\sqrt{\mathbf{5}}}$

com erro absoluto tendendo a zero quando n tende ao infinito.
De fato, temos que

$$\left| f_n - \frac{r^n}{\sqrt{5}} \right| = \frac{|1-r|^n}{\sqrt{5}} \to 0$$

porque $|1 - r| < 1$. Então os números de Fibonacci crescem exponencialmente e, quando n cresce, eles se aproximam dos termos da progressão geométrica

$$\frac{r}{\sqrt{5}}, \frac{r^2}{\sqrt{5}}, \frac{r^3}{\sqrt{5}}, \ldots$$

O número *r*, solução positiva da equação $x^2 = x + 1$, é chamado razão áurea.

EXEMPLO 5
Encontre, diretamente da Fórmula de Binet, o vigésimo número de Fibonacci.
Solução

Temos que $f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$. Desse modo, basta substituir na fórmula de Binet *n* por 20. Assim, $f_{20} = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{20} - \left(\frac{1-\sqrt{5}}{2}\right)^{20}\right]$. Agora, desenvolvemos

$$\left(\frac{1+\sqrt{5}}{2}\right)^{20} = \frac{(1+\sqrt{5})^{20}}{2^{20}} = \frac{(1+\sqrt{5})^{20}}{262144} \quad \text{e} \quad \left(\frac{1-\sqrt{5}}{2}\right)^{20} = \frac{(1-\sqrt{5})^{20}}{2^{20}} = \frac{(1-\sqrt{5})^{20}}{262144}.$$

Pelo Binômio de Newton, o desenvolvimento de $(1+\sqrt{5})^{20} - (1-\sqrt{5})^{20}$ é igual a

$$(1+\sqrt{5})^{20} - (1-\sqrt{5})^{20} = 2\left(\binom{20}{1}\sqrt{5} + \binom{20}{3}(\sqrt{5})^3 + \ldots + \binom{20}{19}(\sqrt{5})^{19}\right).$$

Assim,

$$f_{20} = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{20} - \left(\frac{1-\sqrt{5}}{2}\right)^{20}\right] = \frac{1}{262144\sqrt{5}}\left[2\left(\binom{20}{1}\sqrt{5} + \binom{20}{3}(\sqrt{5})^3 + \ldots + \binom{20}{19}(\sqrt{5})^{19}\right)\right] =$$

$$= \frac{1}{131072}\left[\binom{20}{1} + \binom{20}{3}(\sqrt{5})^2 + \ldots + \binom{20}{19}(\sqrt{5})^{18}\right] =$$

$$= \frac{1}{131072}\left[\binom{20}{1} + \binom{20}{3}.5 + \binom{20}{3}.5^2 + \ldots + \binom{20}{19}.5^9\right] = 6765$$

EXERCÍCIO 5
Usando a Fórmula de Binet, mostre que $f_{2n+1}.f_{2n-1} - f_{2n}.f_{2n+1} = 1$, para todo $n \geq 1$.

2.6 A Fórmula de Lucas para f_n

Os coeficientes do Binômio de Newton (Isaac Newton-1642-1727) $(x + y)^n$, onde n é um número natural, são os $(n+1)$ inteiros da forma $\binom{n}{k} = \frac{n!}{(n-k)!k!}$, $k = 0, 1, 2, 3,..., n$

O *triângulo de Pascal* (Blaisé Pascal- 1623-1662) é formado a partir desses números, fazendo n = 0, 1, 2,... , com k variando de 0 até n, e colocando-se esses números como segue:

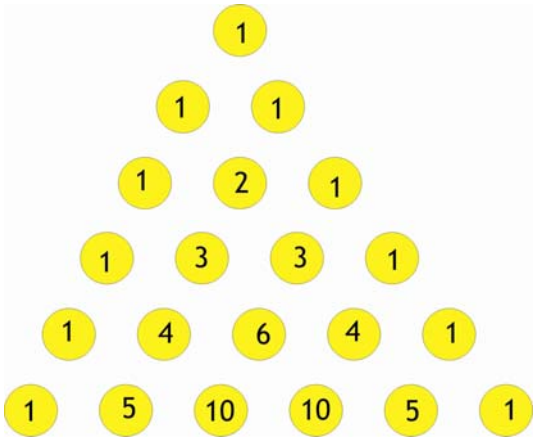

Figura 3 - Triângulo de PASCAL

Se olharmos para o triângulo de Pascal, agora formando um triângulo retângulo, veja a figura 4, a seguir, vamos ver que, surpreendentemente, aparecem aí os números de Fibonacci ([4] pág.135):

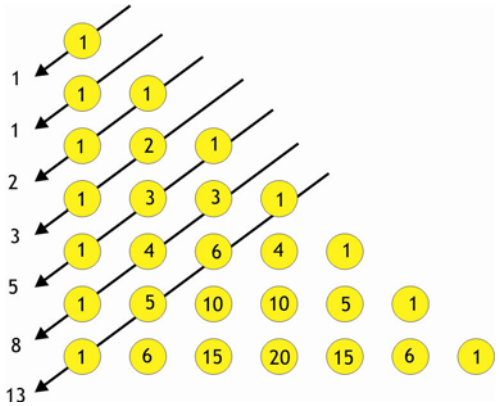

Figura 4 . Triângulo de Pascal, formando um triângulo retângulo

Soma dos elementos das diagonais da figura 4 são os números de Fibonacci: 1, 1, 2, 3, 5, 8, 13, ...

Em 1876, F. Edouard A. Lucas descobriu a seguinte fórmula para os termos de Fibonacci, empregando os coeficientes binomiais:

Teorema 3 (Lucas)

$$f_{n+1} = \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \ldots + \binom{n-j}{j},$$

onde j é o maior inteiro menor do que ou igual a $n/2$.

Demonstração

Por indução sobre *n*.
É fácil ver para os casos n = 0, 1, 2. Suponhamos que a fórmula seja verdadeira para os inteiros 0, 1, 2, 3,..., k-1. Da identidade fundamental e da hipótese de indução temos:

$$f_{k+1} = f_k + f_{k-1} = \left[\binom{k-1}{0} + \binom{k-2}{1} + \binom{k-3}{2} + \ldots + \binom{k-j-1}{j}\right] +$$

$$+ \left[\binom{k-2}{0} + \binom{k-3}{1} + \binom{k-4}{2} + \ldots + \binom{k-j-1}{j-1}\right],$$

que pode ser reescrito como:

$$f_{k+1} = \binom{k-1}{0} + \left[\binom{k-2}{1} + \binom{k-2}{0}\right] + \left[\binom{k-3}{2} + \binom{k-3}{1}\right] + \ldots + \left[\binom{k-j-1}{j} + \binom{k-j-1}{j-1}\right]$$

Agora, aplicando a relação $\binom{m}{i} = \binom{m-1}{i} + \binom{m-1}{i-1}$, obtemos

$$f_{k+1} = \binom{k-1}{0} + \binom{k-1}{1} + \binom{k-2}{2} + \binom{k-3}{3} + \ldots + \binom{k-j}{j}$$

Para concluir a prova, basta observar que a primeira parcela da soma acima é igual à seguinte expressão: $\binom{k}{0}$, para k > 1.

2.7 A Razão Áurea

Considere a razão $r_n = \frac{f_{n+1}}{f_n}$, com n = 1, 2, 3, 4,..., entre os números de Fibonacci consecutivos. A seqüência, r_n, dada por: $\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, \frac{34}{21}, \frac{55}{34}, \ldots.$, possui *propriedades fascinantes*:

(i) os termos de ordem par são decrescentes: $r_2 > r_4 > r_6 > r_8 > r_{10} >> \ldots$.

(ii) os termos de ordem ímpar são crescentes: $r_1 < r_3 < r_5 < r_7 < r_9 <<....$

(iii) os termos consecutivos aparecem em ordem alternada: $r_1 < r_2$, $r_2 > r_3$, $r_3 < r_4$, $r_4 > r_5$,.....

(iv) a seqüência dos intervalos fechados: $[r_1, r_2]$, $[r_3, r_4]$, $[r_5, r_6]$, $[r_7, r_8]$,....., é encaixante, isto é, cada um dos intervalos, a partir do segundo, está inteiramente contido no anterior: $[r_1, r_2] \supseteq [r_3, r_4] \supseteq [r_5, r_6] \supseteq [r_7, r_8] \supseteq$..... . Além disso, o limite do comprimento desses intervalos tende a zero quando n tende ao infinito. De fato, pela identidade de Cassini (veja a Atividade 2 desta Aula) temos: $r_n - r_{n-1} = \frac{(-1)^n}{f_n f_{n-1}}$, que tende para zero quando n tende para infinito.

O Princípio dos Intervalos Encaixantes (que você estudará na disciplina Análise Real) afirma:

Se $I_1, I_2, I_3,...$ é uma seqüência de intervalos fechados e limitados, e se o comprimento de I_n tende a zero quando n tende ao infinito, então existe um, e somente um, número real que pertence a todos os intervalos da seqüência.

Em outras palavras, O Princípio dos Intervalos Encaixantes afirma que o sistema de números reais é *completo*, isto é, sem furo ou brecha ou lacuna.

No caso da seqüência de intervalos fechados definidos acima, concluímos que existe um número real L comum a todo intervalo fechado $[r_{2n-1}, r_{2n}]$, para $n = 1, 2, 3, 4,....$, e, portanto, $L = \lim_{n\to\infty} \frac{f_{n+1}}{f_n}$. Sabendo-se que $f_{n+2} = f_{n+1} + f_n$ e dividindo-se ambos os lados por f_{n+1} temos: $r_{n+1} = 1 + 1/r_n$. Agora, fazendo o limite quando n tende ao infinito, obtemos $L = 1 + \frac{1}{L}$. Portanto, L é a raiz positiva da equação $L^2 = L + 1$, ou seja, $L = \frac{1+\sqrt{5}}{2}$, que é a razão áurea - costumeiramente denotada por τ - e que já havíamos encontrado antes quando estudamos a fórmula de Binet para os números de Fibonacci. Uma aproximação para a razão áurea: $\tau = 1, 6180....$

A *razão áurea* tem origem na antiguidade clássica. Euclides (matemático grego, diretor do famoso Museu de Alexandria e autor de "Os Elementos") chamou-a de "*média e extrema razão"*, que significa a razão obtida quando um segmento de reta está dividido em duas partes desiguais de modo que a razão do todo para o mais largo é igual à razão da maior para a menor:

Figura 5 - Segmento dividido em média e extrema razão

$$\tau = \frac{AB}{AC} = \frac{AC + CB}{AC} = 1 + \frac{CB}{AC} = 1 + \frac{1}{\tau}$$

Na Renascença, a razão áurea era chamada a divina proporção.

A construção clássica de um polígono regular usando somente as ferramentas proposta por Euclides, à régua sem marcação e o compasso, depende da divisão de um segmento de reta na razão τ : 1. Vamos explicar esse fato.
Inicialmente, observe que, para construir um pentágono regular é suficiente construirmos um decágono regular inscrito num circulo, pois o pentágono pode ser formado conectando os vértices do decágono alternadamente. Seguindo o método dos gregos antigos, suponha que o decágono já está construído- portanto o ângulo central AOB, veja Figura 6, a seguir, mede $\frac{2\pi}{10} = \frac{\pi}{5}$. Seja C o ponto sobre o raio OA tal que BC é a bissetriz do ângulo $O\hat{B}A$. Como o triângulo OBA é isóscele, os ângulos da base medem 1/2(π-π/5) = 2π/5. E, portanto, o ângulo OBC mede π/5. O ângulo ACB, que é externo, mede π/5 + π/5= 2π/5. Logo, os triângulos ABC e OBC são também isósceles. Portanto: OC = BC = AB.

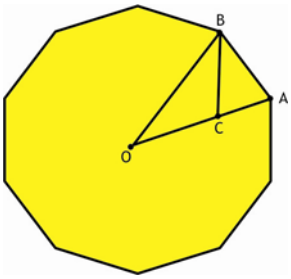

Figura 6 - Construção de um decágono inscrito num círculo

Tomando o raio do círculo medindo 1, o lado do decágono AB = x, e como os triângulos ABO e ABC são semelhantes, por terem os mesmos ângulos, temos: $\frac{1}{x} = \frac{x}{1-x}$. Portanto, o ponto C divide o raio em média e extrema razão. Segue que: $\frac{1}{x} = \tau \Rightarrow x = \frac{1}{\tau} \Rightarrow x = \frac{2}{\sqrt{5}+1} = \frac{2}{\sqrt{5}+1}.\frac{\sqrt{5}-1}{\sqrt{5}-1} = \frac{\sqrt{5}-1}{2}$. Como o segmento de comprimento $\sqrt{5}$ pode ser construído, usando somente a régua e o compasso, também podemos construir o lado do decágono.

Exercícios

1) Mostre que a soma $f_n^2 + f^2_{n+1}$ é sempre um número de Fibonacci.

2) Mostre que $f_1 f_2 + f_2 f_3 + +... + f_{2n-1} f_{2n} = f^2_{2n}$

3) Encontre fórmulas simples para as somas
   (a) $f_1 + f_3 + f_5 + ... + f_{2n-1}$

(b) $f_2 + f_4 + f_6 + ... + f_{2n}$

4) De quantas maneiras é possível subir uma escada com n degraus pisando em um ou dois degraus de cada vez?

5) Prove que:
(a) se 2 divide f_{n+1} então 4 divide $(f_n^2 - f_{n-1}^2)$
(b) se 3 divide f_n, então 9 divide $(f_{n+1}^3 - f_{n-1}^3)$

6) Prove que: $(f_n\ f_{n+3})^2 + (2f_{n+1}\ f_{n+2})^2 = (f_{2n+3})^2$ e use isso para gerar 5 triplas Pitagóricas, isto é, números que satisfazem ao Teorema de Pitágoras (o quadrado do maior número é igual à soma dos quadrados dos outros dois).

7) Prove que o produto $f_n\ f_{n+1}\ f_{n+2}\ f_{n+3}$, de quaisquer quatro números de Fibonacci consecutivos é igual à área de um triângulo retângulo de lados inteiros (triângulo pitagórico).

8) Mostre que a soma dos quadrados dos primeiros n números de Fibonacci é igual à $f_n f_{n+1}$.

9) Mostre que a diferença $f^2_{n+1} - f^2_{n-1}$ é um número de Fibonacci, para todos $n \geq 2$.

10) Verificar que:
(a) 2 divide f_n se, e somente se, 3 divide n.
(b) 3 divide f_n se, e somente se, 4 divide n.
(c) 4 divide f_n se, e somente se, 6 divide n.
(d) 5 divide f_n se, e somente se, 5 divide n.

RESUMO

Nesta aula, introduzimos as seqüências de Fibonacci, que foram usadas no século VIII para descrever métricas na poesia sânscrita e que apareceram pela primeira vez na Europa em 1202, através do livro Líber Abaci, de Leonardo de Pisa, mais conhecido como Fibonacci. Posteriormente, em 1634, Albert Girard, matemático alemão e aluno de Viète, definiu a seqüência de Fibonacci recursivamente.

REFERÊNCIAS

BURTON, DAVID M., **Elementary number theory** – 4 th ed. The McGraw-Hill Companies, Inc. New York. 1998

de CARVALHO, JOÃO. B. P., **Euclides, Fibonacci e Lamé,**
RPM- SBM, No. 24, 32-40. Rio de Janeiro. 1993

STRUICK, DIRK, J., **História Concisa das Matemáticas**. Gradiva. Lisboa. 1989

YOUNG, ROBERT M., **Excursions Calculus : An Interplay of The Continous and the Discrete**. Dolciani Mathematical Exposition, MAA, Washington. 1992

ZECKENDORF, E., **Representation des nombres natureals par une somme de nombres de Fibonacci ou de nombres de Lucas.** Bull. de la Soc. Royale des Sci. de Liege, 41 (1972) 179-182. França.

Aula 11 – Noções sobre o processo e o método de criptografar

Apresentação

Esta é a Aula 09 da disciplina **Métodos e Modelos Matemáticos**, que estuda aplicações da Matemática no cotidiano das pessoas. Aqui você estudará como usar fatos simples da disciplina de Teoria dos Números para criar seus próprios códigos secretos de comunicação. Também, veremos como os sites de venda de produtos pela INTERNET fazem para tornar as vendas seguras, para quem usa o cartão de crédito.

Nesta aula, damos uma idéia de como se usou a Matemática no passado e como se usa nos dias atuais para codificar e descodificar mensagem, visando atender necessidades do dia-a-dia.

Tente entender tudo que está sendo explicado na aula. Estude com caneta e papel ao lado. Seja paciente e procure ter certeza de que você entendeu o que (e por que) está fazendo.

Objetivos

- Usar a Matemática para resolver problemas do cotidiano.
- Usar a Teoria dos Números para resolver problemas de tornar senhas ou mensagens seguras, de modo que sejam somente conhecidas pelos seus donos ou usuários credenciados.

1. Noções básicas de Criptografia

Criptografia, palavra que vem do grego e kryptós, "secreto", e gráphein, "escrita", é o estudo dos princípios, técnicas e implementação de sistemas sigilosos pelos quais a informação pode ser transformada da sua forma original para outra ilegível, de maneira que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado, de modo que só o receptor da mensagem pode ler a informação com facilidade.

A procura pelo uso da criptografia é proporcional a necessidade de passar ou receber informações consideradas sigilosas para um indivíduo, grupo de pessoas, comércio, organizações civis ou militares etc.

Este tipo de procedimento tem suas origens nos babilônios, egípcios e hindus.

Pesquisadores encontraram inscrições cuneiformes, datadas de 1500 a. C., contendo procedimentos criptografados para fazer cerâmica esmaltada.

O historiador grego Heródoto, em seu "A História", que é um relato sobre a guerra entre gregos e persas, conta que, no ano de 499 a. C., Histiaeus, tirano de Miletos, raspou a cabeça de um escravo e tatuou uma mensagem para ser usada na guerra contra a Pérsia. Depois que o cabelo do escravo cresceu, Histiaeus enviou o mesmo para seu genro Aristágoras, em Miletos, que após raspar a cabeça do escravo encontrou a mensagem.

Polybius, político, diplomata e historiador grego do período helenístico, no segundo século antes de Cristo, criou um sistema criptográfico que substituía as letras de um texto por um par de números. Olhando com nosso alfabeto atual, o procedimento de Polybius seria dispor as letras do alfabeto da esquerda para direita e de cima para baixo em um tabuleiro 5 por 5, de modo que as letras I e J são combinadas para ficar numa mesma posição. Cada letra era substituída por um par de dígitos, de maneira que o primeiro representava a linha em que a letra se encontrava e o segundo a coluna, veja Tabela I, a seguir.

Tabela I

	1	**2**	**3**	**4**	**5**
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

De acordo com o método de Polybius, a mensagem "O HOMEM VAI HOJE" seria enviada como: 34 23 34 32 15 32 51 11 24 23 34 24 15.

Outro exemplo de mensagem criptografada, um criptograma, é baseado na transformação de cada letra do texto em outra letra diferente, para produzir assim a escrita secreta. Pesquisadores descobriram um criptograma usado por Júlio César, imperador romano, que se usado com o nosso alfabeto atual, com 26 letras, substituía cada letra pela letra que estivesse, na ordem usual do alfabeto, três letras depois, sendo que as três últimas X, Y e Z eram substituídas por A, B e C, respectivamente, veja na Tabela II, a seguir.

Tabela II

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Deste modo, a mensagem "FELIZ NATAL" seria criptografada como: "IHOLCQDWDO"

EXEMPLO 1
Usando o método de Polybius, faça o criptograma da mensagem seguinte:

"ENVIE TROPAS"

SOLUÇÃO

Usando a Tabela 1, temos: E N V I E T R O P A S
15 33 51 24 15 44 42 34 35 11 43

EXERCÍCIO 1
Usando o método de Polybius, decifre a mensagem:

45 43 11 42 15 24 34 12 11 42 13 34

Associando a cada letra do alfabeto um número, de acordo com a Tabela III, a seguir, podemos construir um criptograma baseado na noção de congruência.

Tabela III

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Seja Y o correspondente numérico de uma letra num texto, como na Tabela III acima, e seja X o equivalente numérico da letra correspondente no texto criptografado. No

sistema usado por Júlio César, teríamos $X \equiv Y + 3 \pmod{26}$. No momento de decifrar uma mensagem, basta usar a congruência $Y \equiv X - 3 \pmod{26}$.

EXEMPLO 2

Seja Y o correspondente numérico de uma letra num texto, como na Tabela III acima, e seja X o equivalente numérico da letra correspondente no texto criptografado, de tal modo que $X \equiv Y + 15 \pmod{26}$. Use este criptograma para transformar a mensagem:

"ENVIE REFORÇOS"

numa mensagem numérica.

SOLUÇÃO

Para criptografar a mensagem, transformando-a numa mensagem numérica, temos que saber qual será o número que corresponde a cada letra do texto-mensagem dado.
Assim, o número que corresponderá à letra E será o número da Tabela II acima, representado pela incógnita X, satisfazendo:

$$X \equiv E + 15 \pmod{26} = 4 + 15 \pmod{26} = 19 \pmod{26}.$$

Ou seja $X = 19$.
O número que corresponderá à letra N será aquele da Tabela II acima, representado pela incógnita X, tal que:

$X \equiv N + 15 \pmod{26} = 13 + 15 \pmod{26} = 28 \pmod{26} = 2 \pmod{26}$, ou seja $X = 2$.

O número que corresponderá à letra V será aquele da Tabela II acima, representado pela incógnita X, tal que

$X \equiv V + 15 \pmod{26} = 21 + 15 \pmod{26} = 36 \pmod{26} = 10 \pmod{26}$, ou seja $X = 10$.

O número que corresponderá à letra I será aquele da Tabela II acima, representado pela incógnita X, tal que

$$X \equiv I + 15 \pmod{26} = 8 + 15 \pmod{26} = 23 \pmod{26}, \text{ ou seja } X = 23.$$

O número que corresponderá à letra R será aquele da Tabela II acima, representado pela incógnita X, tal que

$X \equiv R + 15 \pmod{26} = 17 + 15 \pmod{26} = 32 \pmod{26} = 6 \pmod{26}$, ou seja $X = 6$.

O número que corresponderá à letra F será aquele da Tabela II acima, representado pela incógnita X, tal que

$$X \equiv F + 15 \pmod{26} = 5 + 15 \pmod{26} = 20 \pmod{26}, \text{ ou seja } X = 20.$$

O número que corresponderá à letra O será aquele da Tabela II acima, representado pela incógnita X, tal que

$X \equiv O + 15 \pmod{26} = 14 + 15 \pmod{26} = 29 \pmod{26} = 3 \pmod{26}$, ou seja $X = 3$.

O número que corresponderá à letra Ç (usamos o mesmo que a letra C) será aquele da Tabela II acima, representado pela incógnita X, tal que

$$X \equiv C + 15 \pmod{26} = 3 + 15 \pmod{26} = 18 \pmod{26}, \text{ ou seja } X = 18.$$

O número que corresponderá à letra S será aquele da Tabela II acima, representado pela incógnita X, tal que

$$X \equiv S + 15 \pmod{26} = 18 + 15 \pmod{26} = 33 \pmod{26} = 7 \pmod{26}, \text{ ou seja } X = 7.$$

Portanto, a mensagem numérica será: 192102319 6192031837.

EXERCÍCIO 2

Seja Y o correspondente numérico de uma letra num texto, como na Tabela III acima, e seja X o equivalente numérico da letra correspondente no texto criptografado, de tal modo que $X \equiv Y + 19 \pmod{26}$. Use este criptograma para transformar a mensagem:

"HOJE CHOVEU MUITO"

numa mensagem numérica.

Generalizando o que vimos acima, podemos construir criptogramas usando a congruência

$$X \equiv aY + b \pmod{26}$$

onde a, b são inteiros não negativos e menores do que ou iguais a 25, tendo a condição MDC $(a, 26) = 1$.

A condição MDC $(a, 26) = 1$ é para garantir que podemos encontrar o Y, quando estivermos no processo de descodificação da mensagem, ou seja, transformando-a num modo legível usual.
Vejamos como isso é feito.
O fato de que MDC $(a, 26) = 1$, implica que existem inteiros m e n tais que $am + 26n = 1$. Portanto, módulo 26, a equação diofantina $am + 26n = 1$ dá origem a congruência $am \equiv 1 \pmod{26}$, o que significa dizer que a é invertível módulo 26, para todo inteiro $a \in \{1, 2, 3, ..., 25\}$. Deste modo, se você está lendo uma mensagem codificada segundo a congruência $X \equiv aY + b \pmod{26}$, você pode obter o valor de Y da forma seguinte:

$X \equiv aY + b \pmod{26} \Rightarrow X - b \equiv aY \pmod{26} \Leftrightarrow aY \equiv X - b \pmod{26} \Rightarrow$ $\mathbf{Y \equiv a^{-1}(X - b) \pmod{26}}$.

Portanto, para trabalhar com a congruência $X \equiv aY + b \pmod{26}$, temos 26 escolhas para o inteiro b, de 0 até 25, e $\varphi(26) = 12$ escolhas para o número inteiro a, onde φ é a função de Euler.
Veja na Tabela IV, a seguir, os possíveis valores de a e seus inversos.

Tabela IV

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1} módulo 26	1	9	21	15	13	19	7	23	11	5	17	25

EXEMPLO 3
Transformar a mensagem-texto "ESTAREI NA PONTE" numa mensagem numérica usando a congruência $X \equiv 9Y + 15 \pmod{26}$.
SOLUÇÃO

Para criptografar a mensagem, transformando-a numa mensagem numérica, temos que saber qual será o número que corresponde a cada letra do texto-mensagem dado.
Como a letra E na Tabela II corresponde ao número 4, o número que vai corresponder à letra E será o número X tal que

$$X \equiv 9.4 + 15 \pmod{26} = 36 + 15 \pmod{26} = 51 \pmod{26} \equiv 25 \pmod{26}.$$

Portanto, a letra E será representada pelo número 25.
Como a letra S na Tabela II corresponde ao número 18, o número que vai corresponder à letra S será o número X tal que

$$X \equiv 9.18 + 15 \pmod{26} = 162 + 15 \pmod{26} = 177 \pmod{26} \equiv 21 \pmod{26}.$$

Portanto, a letra S será representada pelo número 21.
Como a letra T na Tabela II corresponde ao número 19, o número que vai corresponder à letra T será o número X tal que

$$X \equiv 9.19 + 15 \pmod{26} = 171 + 15 \pmod{26} = 186 \pmod{26} \equiv 4 \pmod{26}.$$

Portanto, a letra T será representada pelo número 4.
Como a letra A na Tabela II corresponde ao número 0, o número que vai corresponder à letra A será o número X tal que

$$X \equiv 9.0 + 15 \pmod{26} = 0 + 15 \pmod{26} = 15 \pmod{26} \equiv 15 \pmod{26}.$$

Portanto, a letra A será representada pelo número 15.
Como a letra R na Tabela II corresponde ao número 17, o número que vai corresponder à letra R será o número X tal que

$$X \equiv 9.17 + 15 \pmod{26} = 153 + 15 \pmod{26} = 168 \pmod{26} \equiv 22 \pmod{26}.$$

Portanto, a letra R será representada pelo número 22.

Como a letra I na Tabela II corresponde ao número 8, o número que vai corresponder à letra I será o número X tal que

$$X \equiv 9.8 + 15 \pmod{26} = 72 + 15 \pmod{26} = 87 \pmod{26} \equiv 9 \pmod{26}.$$

Portanto, a letra I será representada pelo número 9.
Como a letra N na Tabela II corresponde ao número 13, o número que vai corresponder à letra N será o número X tal que

$$X \equiv 9.13 + 15 \pmod{26} = 117 + 15 \pmod{26} = 132 \pmod{26} \equiv 2 \pmod{26}.$$

Portanto, a letra N será representada pelo número 2.
Como a letra P na Tabela II corresponde ao número 15, o número que vai corresponder à letra P será o número X tal que

$$X \equiv 9.15 + 15 \pmod{26} = 135 + 15 \pmod{26} = 150 \pmod{26} \equiv 20 \pmod{26}.$$

Portanto, a letra T será representada pelo número 20.
Como a letra O na Tabela II corresponde ao número 14, o número que vai corresponder à letra O será o número X tal que

$$X \equiv 9.14 + 15 \pmod{26} = 136 + 15 \pmod{26} = 151 \pmod{26} \equiv 21 \pmod{26}.$$

Portanto, a letra O será representada pelo número 21.

Assim, a mensagem "ESTAREI NA PONTE" será transformada na seguinte mensagem numérica: 25 21 4 15 2 25 9 2 15 20 21 24 25.

EXERCÍCIO 3
(a) Transformar a mensagem-texto "FELIZ NATAL" numa mensagem numérica usando a congruência $X \equiv 21Y + 7 \pmod{26}$.
(b) Verifique que sua resposta está correta, ou seja, confirme que a mensagem numérica encontrada no subitem (a) é de fato "FELIZ NATAL".

Um criptograma semelhante aos estudados acima oferece a possibilidade para uma pessoa decifrá-lo sem grandes investimentos. Isto acontece porque a freqüência média com que cada letra (de uma dada língua, no nosso caso o português) aparece em algum texto é mais ou menos constante. De modo que, contando a freqüência de aparecimento de cada símbolo no texto criptografado, é possível descobrir a que letra ele corresponde. É bem verdade que, existem maneiras de complicar bastante o processo de identificação de cada letra na mensagem codificada. Por exemplo, usar um processo que destrói a estrutura da frase, subdividindo a mensagem em blocos de letras e embaralhando esses blocos. É possível fazer isso eliminando os espaços entre blocos de palavras, subdividindo a mensagem em blocos de duas letras, permutando os blocos, trocando o primeiro pelo último, o segundo pelo penúltimo etc. Mas, estes passos que dificultam a identificação dos dados por estranhos, concorrentes ou pessoas com más intenções,

apresentam desvantagem nas aplicações comerciais, que normalmente são feitas através de computadores. O fato é que estes cuidados deixariam o processo extremamente lento.

Em 1977, três pesquisadores que trabalhavam no Massachussets Institute of Tecnology –MIT, nos Estados Unidos, R. L. Rivest, A Shamir e L. Adleman, idealizaram um método de codificar números, que ficou conhecido como RSA, que é simples de fazer, mas muito difícil de desfazer, adaptando-se perfeitamente para as transações comercias, com segurança e rapidez. No próximo parágrafo, vamos ter uma noção de como esta brilhante idéia pode ser colocada em prática, com constantes aperfeiçoamentos.

2. CRIPTOGRAFIA RSA

Um problema importante para os nossos propósitos é o seguinte:

Problema Dado um número natural K, K é primo ou não?

Você aprendeu, na disciplina de Teoria dos Números, o conhecido Pequeno Teorema de Fermat:

K é um número primo $\Rightarrow a^K \equiv a \pmod{K}$, para todo inteiro a, com $1 \leq a \leq K - 1$.

Podemos aplicar o Pequeno Teorema de Fermat para decidir se K é primo ou não.

Como faremos isto?

Inicialmente, poderíamos fazer as divisões de K por um dos primos 2, 3, 5, 7, ...,. Se K for divisível por um desses, então K não é primo. Caso contrário, continuaria o processo de divisão pelos primos seguintes. Este método **pode ser longo** e não talvez não consigamos uma resposta a curto ou em médio prazo.

Outra maneira de verificar se K é primo, seria verificar se $2^K \equiv 2 \pmod{K}$. Se não acontece isso, poderemos concluir, pelo Pequeno Teorema de Fermat, que o número K é composto. Se, por outro lado, se tivermos $2^K \equiv 2 \pmod{K}$, então há uma chance de K ser primo. Neste caso, verificaríamos se $3^K \equiv 3 \pmod{K}$. Se isto não acontece, então K é composto. Caso contrário, há uma chance de K ser primo. Continuando este processo para 5, 7, 11, 13, 17, ... , podemos tirar uma conclusão: ou K é composto ou K é primo.

Observe que, podemos escolher, aleatoriamente, um número inteiro $a < K$ e verificar a congruência $a^K \equiv a \pmod{K}$. Se esta congruência não ocorre, então K não é primo. Um computador pode fazer este teste em poucos minutos, se o número não for arbitrariamente grande. Agora, o computador, mesmo os mais velozes, no entanto, sabendo que K não é primo, levaria anos para conhecer seus fatores primos. Ou seja, podemos em pouco tempo saber se o número K é primo, mas, se ele não é primo, levaríamos muito tempo para conhecer seus fatores primos, p e q, de modo que $K = p.q$.

Esta é a idéia da criptografia RSA.

Escolhe-se dois números primos grandes, p e q, de preferência com mais de cem dígitos, define-se $K = p.q$. Cada pessoa que utiliza o sistema escolhe um inteiro positivo s, tal que $MDC(s, \varphi(K)) = 1$, e dois inteiros t e u tal que $st = 1 + u\varphi(K)$. Portanto, $st \equiv 1 \pmod{\varphi(K)}$. O par (K, s) é o par que é tornado público para os usuários do sistema, mas o número t, a chave que decifra, fica secretamente guardada.

O que vimos acima, só tratou de números. Mas, muitas mensagens são mensagens-texto. Então, para usar o sistema RSA, temos que estabelecer uma maneira de converter a mensagem-texto em uma sequência de números.

No sistema RSA, cada letra é convertida em um par de números, de acordo com a Tabela IV, a seguir.

Tabela V

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Para usar o sistema RSA, transformamos a mensagem-texto numa mensagem numérica, usando a Tabela V. Os blocos numéricos Y, obtidos pela transformação da mensagem-texto em mensagem-numérica, usando a Tabela V, são codificados, como X, usando o número s e a congruência $X \equiv Y^s \pmod{K}$, onde $0 \leq X < K$, e o texto criptografado é enviado.
Usando o Teorema de Fermat, na versão do Teorema de Euler, temos que
$Y^{\varphi(K)} \equiv 1 \pmod{K}$. Portanto, podemos escrever:
$X^t \equiv (Y^s)^t \pmod{K} = Y^{st} \pmod{K} = Y^{1 + u\varphi(K)} \pmod{K} = Y.Y^{u\varphi(K)} \pmod{K} \equiv Y \pmod{K}$
com $0 < Y < K$.
Podemos escolher o número s como sendo qualquer primo maior do que $K = p.q$, tal que $2^s > K = p.q$, e seria impossível recuperar a mensagem-texto, Y, simplesmente calculando a raiz s-ésima de X^t. Logo, o conhecimento do par (K, s) não leva uma pessoa a conhecer o par decifrador (t, K). Na verdade, para obter t, o inverso de s módulo $\varphi(K)$, temos primeiro que determinar $\varphi(K) = \varphi(p.q) = (p - 1).(q - 1)$, que requer que o decifrador conheça a fatoração de K, que é praticamente impossível sem conhecer p e q.

EXEMPLO 4
(a) Usando o sistema RSA, para $p = 61$, $q = 47$, $K = p.q = 61.47 = 2867$ e $s = 17$, codifique a mensagem: "O ENCONTRO SERÁ HOJE"
(b) Imagine que você recebeu a seguinte mensagem
1404 1562 0425 2251 0408 2137 0078 1819
codificada pelo método RSA, com os mesmos parâmetros do subitem (a) e você conhece o parâmetro t = 2273.
Decifre a mensagem recebida
SOLUÇÃO

Temos que $\varphi(K) = \varphi(61).\varphi(47) = 60.46 = 2760$.

Agora, temos que encontrar t, que é o inverso de $s = 17$ módulo K = 2867. Para isso, temos que $st \equiv 1 \pmod{\varphi(K)}$, ou seja $17t \equiv 1 \pmod{2760}$, que é o mesmo que a equação diofantina $17t - 2760u = 1$. Assim, usando o Algoritmo da Divisão, temos:
$-2760 = (-163).17 + 11$; $17 = 1.11 + 6$; $11 = 1.6 + 5$; $6 = 1.5 + 1$.
Assim, $1 = 6 + 5(-1) = 6 + [11 + 6(-1)](-1) = 11(-1) + 6.2 = 11.(-1) + [17 + 11(-1)].2$, que é mesmo que :
$1 = 17.2 + 11(-3) = 17.2 + [-2760 + 17.163](-3) = 17.2 + 2760.3 + 17(-489)$, que nos dá:
$1 = 17.(-487) + 2760.3 = 17.(-487) - 2760(-3)$.
Assim, módulo 2760, temos $17.(-487) \equiv 1 \pmod{2760}$. Mas, $-487 \equiv 2273 \pmod{2760}$.
Portanto, $17.2273 \equiv 1 \pmod{2760}$, e o inverso de $s = 17$ é $t = 2273$.
Agora, usando a Tabela V, transformamos a mensagem texto na mensagem numérica equivalente, agrupando os números em blocos de 4:

1404 1502 1413 1917 1418 0417 0014 0904,

Usamos a congruência $X \equiv Y^s \pmod{K}$, que neste caso é $X \equiv Y^{17} \pmod{2867}$, para codificar a mensagem numérica. Logo, basta fazer o cálculo $Y^{17} \pmod{2867}$, para $Y \in \{1404, 1502, 1413, 1917, 1418, 0417, 0014, 0904\}$. Assim, temos:

$1404^{17} \equiv 1526 \pmod{2867}$
$1502^{17} \equiv 1562 \pmod{2867}$;
$1413^{17} \equiv 425 \pmod{2867}$;
$1917^{17} \equiv 2251 \pmod{2867}$;
$1418^{17} \equiv 408 \pmod{2867}$;
$0414^{17} \equiv 2137 \pmod{2867}$;
$0014^{17} \equiv 780 \pmod{2867}$;
$0904^{17} \equiv 1819 \pmod{2867}$.

Portanto, a mensagem "O ENCONTRO SERÁ HOJE" será codificada como:

1526 1562 0425 2251 0408 2137 0078 1819

(b) Pelo exposto acima, para ler a mensagem dada, vamos usar a congruência:
$X^t \equiv (Y^s)^t \pmod{K} = Y^{st} \pmod{K} = Y^{1 + u\varphi(K)} \pmod{K} = Y.Y^{u\varphi(K)} \pmod{K} \equiv Y \pmod{K}$
com $t = 2273$ e $0 < Y < K = 2867$, para decifrar a mensagem. No caso, $X \in \{1526, 1562, 0425, 2251, 0408, 2137, 0780, 1819\}$. Assim, temos:

$1526^{2273} \equiv 1404 \pmod{2867}$;
$1562^{2273} \equiv 1562 \pmod{2867}$;
$0425^{2273} \equiv 1413 \pmod{2867}$;
$2251^{2273} \equiv 1917 \pmod{2867}$;
$0408^{2273} \equiv 1418 \pmod{2867}$;
$2137^{2273} \equiv 0414 \pmod{2867}$;
$0780^{2273} \equiv 0014 \pmod{2867}$;
$1819^{2273} \equiv 0904 \pmod{2867}$;

E a mensagem numérica seria 1404 1502 1413 1917 1418 0417 0014 0904, que corresponde, exatamente, a mensagem do subitem (a). Na verdade, o que fizemos foi

mostrar que o método realmente funciona, verificando como decifrar uma mensagem codificada que já sabíamos qual era.

EXERCÍCIO 4

(a) Usando o sistema RSA, para $p = 83$, $q = 97$, $K = p.q = 83.97 = 8051$ e $s = 29$, codifique a mensagem: "O LIVRO CHEGOU".

(b) Verifique que a sua resposta está correta, fazendo os cálculos semelhantes às do subitem (b) do Exemplo 4, acima.

É oportuno observar que, o fato de alguém conhecer K e s, não o leva a encontrar t, pois para ter o valor de t, que é o inverso de s módulo $\varphi(K)$, teria que determinar $\varphi(K)$, que sabemos ser $\varphi(K) = \varphi(p.q) = (p - 1).(q - 1)$. Mas, para isso, precisaria conhecer a fatoração de K, o que é praticamente impossível sem conhecer os fatores p e q.

Agora, se alguém conhece K e $\varphi(K)$, os fatores p e q podem ser conhecidos. De fato, usando a identidade: $(p-q)^2 - (p+q)^2 = -4pq$ e, também, o fato de que

$$p + q = pq - (p-1).(q-1) + 1 = pq - \varphi(K) + 1, \text{ e a igualdade}$$

$$(p - q) = [(p+q)^2 - 4pq]^{1/2} = [(p+q)^2 - 4K]^{1/2}, \text{ teremos:}$$

$$p = \frac{(p+q)+(p-q)}{2} \quad e \quad q = \frac{(p+q)-(p-q)}{2}$$

EXEMPLO 5

Determine os primos p e q, usados no sistema RSA dado por $K = 4386607$ e $\varphi(K) = 4382136$.

SOLUÇÃO

Temos que $K = p.q$ e $\varphi(K) = 4382136$. Pelos cálculos feitos acima, temos que:

$$p + q = pq - \varphi(K) + 1 = 4386607 - 4382136 + 1 = 4472 \quad e$$

$$p - q = [(p+q)^2 - 4K]^{1/2} = [4472^2 - 4 \times 4386607]^{1/2} = 1566.$$

Portanto, temos que:

$$p = \frac{(p+q)+(p-q)}{2} = \frac{\mathbf{4472+1566}}{\mathbf{2}} = \mathbf{3019} \qquad e$$

$$q = \frac{(p+q)-(p-q)}{2} = \frac{\mathbf{4472-1566}}{\mathbf{2}} = \mathbf{1453}$$

FIM DO EXEMPLO

EXERCÍCIO 5

Usando o sistema RSA usado no Exemplo 5, a cima, e sabendo que $s = 5$, calcule o valor de t.

EXERCÍCIOS

1) Use o sistema de Polybius para codificar a mensagem "ASA BRANCA".

2) Use o sistema de Julio César, imperador romano, para codificar a mensagem-texto: "O SOL BRILHARÁ PARA TODOS".

3) Transformar a mensagem-texto "ESTADO DO RIO GRANDE DO NORTE" numa mensagem numérica usando a congruência $X \equiv 21Y + 7 \pmod{26}$.
(b) Verifique que sua resposta está correta, ou seja, confirme que a mensagem numérica encontrada no subitem (a) é de fato "ESTADO DO RIO GRANDE DO NORTE".

4)Determine dois números primos p e q usados no sistema RSA, sabendo-se que $K = 4386607$ e $\varphi(K) = 4382136$. Se $s = 5$ determine t.

Resumo

Nesta aula estudamos alguns sistemas usados para criptografar mensagens-textos. Particularmente, vimos qual é a idéia do sistema RSA.

Referências

COUTINHO, S. C. **Números Inteiros e Criptografia RSA.** Rio de Janeiro, IMPA/SBM, 1997.

COUTINHO, S. C. **Criptografia.** Rio de Janeiro, IMPA/SBM, Programa de Iniciação Científica da OBMEP. 2007.

HEFEZ, Abramo. **Elementos de aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2005.

TATTERSALL, James J. **Elementary Number Theory in Nine Chapters**. Cambridge University Press. Cambridge. New York. 1999.